Universidad Nacional Mayor de San Marcos
Universidad del Perú. Decana de América

Dirección General de Estudios de Posgrado
Facultad de Ciencias Matemáticas
Unidad de Posgrado

Unicidad de los cuaterniones y octoniones como R-algebras de división y sus representaciones matriciales

TESIS

Para optar el Grado Académico de Magíster en Matemática Pura

AUTOR

Marco Antonio RUBIO GALLARDAY

ASESOR

Mg. Víctor Hilario TARAZONA MIRANDA

Lima, Perú

2019

Referencia bibliográfica

Rubio, M. (2019). *Unicidad de los cuaterniones y octoniones como R-algebras de división y sus representaciones matriciales*. Tesis para optar grado de Magíster en Matemática Pura. Unidad de Posgrado, Facultad de Ciencias Matemáticas, Universidad Nacional Mayor de San Marcos, Lima, Perú.

HOJA DE METADATOS COMPLEMENTARIOS

CODIGO ORCID DEL AUTOR: 0000-0002-8459-0989

CODIGO ORCID DEL ASESOR: 0000-0001-6444-8793

DNI: 09264893

GRUPO DE INVESTIGACIÓN:

INSTITUCIÓN QUE FINANCIA PARCIAL O TOTALMENTE LA INVESTIGACIÓN: Autofinanciado

UBICACIÓN GEOGRÁFICA DONDE SE DESARROLLÓ LA INVESTIGACIÓN. DEBE INCLUIR LOCALIDADES Y COORDENADAS GEOGRÁFICAS

Campus: Ciudad Universitaria (Av. Universitaria s/n – Av. Venezuela cdra. 34, Lima Perú) Coordenadas: 120 03’ 30’’S 770 05’ 00’’O

AÑO O RANGO DE AÑOS QUE LA INVESTIGACIÒN ABARCÓ:

2013 - 2019

ACTA DE SUSTENTACIÓN DE TESIS DE GRADO ACADÉMICO DE MAGÍSTER

Siendo las, ... horas del día viernes veinte de diciembre del dos mil diecinueve, en el Auditorio de la Facultad de Ciencias Matemáticas, el Jurado Evaluador de Tesis, Presidido por el Mg. Wilfredo Mendoza Quispe e integrado por los siguientes miembros, Dr. Pedro Celso Contreras Chamorro (Jurado Evaluador), Mg. William César Olano Díaz (Jurado Informante) y el Mg. Víctor Hilario Tarazona Miranda como Miembro Asesor, se reunieron para la sustentación de la tesis titulada: «UNICIDAD DE LOS CUATERNIONES Y OCTONIONES COMO R-ALGEBRAS DE DIVISIÓN Y SUS REPRESENTACIONES MATRICIALES» presentada por el Bachiller Marco Antonio Rubio Gallarday para optar el Grado Académico de Magíster en Matemática Pura.

Luego de la exposición del graduando, los Miembros del Jurado hicieron las preguntas correspondientes, así como las observaciones e inquietudes acerca del trabajo de tesis, a las cuales el Bachiller Marco Antonio Rubio Gallarday respondió con acierto y solvencia, demostrando pleno conocimiento del tema.

A continuación se realizó la calificación correspondiente, según tabla adjunta, resultando el Bachiller Marco Antonio Rubio Gallarday aprobado con el calificativo de ..MUY... BUENO..(18)

Habiendo sido aprobada la sustentación de la Tesis, el Jurado Evaluador recomienda para que el Consejo de Facultad apruebe el otorgamiento del Grado Académico de **Magíster en Matemática Pura al Bachiller Marco Antonio Rubio Gallarday**.

Siendo las 17:00 horas, se levantó la sesión, firmando para constancia la presente Acta.

Dr. Pedro Celso Contreras Chamorro
Miembro

Mg. Wilfredo Mendoza Quispe
Presidente

Mg. William César Olano Díaz
Miembro

Mg. Víctor Hilario Tarazona Miranda
Miembro Asesor

Agradecimientos

- Al Mg. Víctor Tarazona Miranda por motivarme para la realización de esta tesis.
- Mi eterna gratitud al Dr. Pedro Contreas Chamorro por sus valiosas observaciones, sugerencias y su apoyo incondicional para la culminación de la presente tesis.

RESUMEN

Unicidad de los cuaterniones y octoniones como $\mathbb{R}$-Álgebras de división y sus representaciones matriciales

En el presente trabajo estudiaremos la teoría de las álgebras reales de división, los resultados de Hopf, Frobenius y de las álgebras alternativas cuadráticas. Estos resultados nos permitirán justificar desde el punto de vista de los fundamentos de la matemática la unicidad de estas álgebras, la representación matricial de los cuaterniones y exhibir una representación " matricial" de los octoniones.

El trabajo consta de tres capítulos. En el primer capítulo proporcionamos algunos conceptos y algunos resultados de las álgebras reales y de topología.

En el capítulo dos, probamos que toda álgebra real conmutativa de divisón de dimensión finita tiene dimensión menor o igual a dos. Describimos el álgebra de los cuaterniones y exhibimos una representación matricial de está álgebra. Estudiamos algunos resultados de las álgebras alternativas que nos permiten probar que toda álgebra real $\mathcal{A} \neq 0$ asociativa, cuadrática sin divisores de cero de dimensión mayor que dos es isomorfa al álgebra de los cuaterniones.

En el tercer capítulo estudiamos algunos resultados de las álgebras alternativas cuadráticas, que nos permitan describir el álgebra de los octoniones. Probamos que toda álgebra real alternativa, cuadrática sin divisores de cero y no asociativa es isomorfa al álgebra de los octoniones. Finalmente proporcionamos una representación una representación " matricial" de los octoniones.

Palabras clave:

- Álgebra sin divisores de cero.
- Álgebra alternativa
- Álgebra cuadrática

ABSTRACT

Uniqueness of the quaternions and octonions as $\mathbb{R}$ division algebras and their matrix representations

In the present work we will study the theory of real division algebras, the results of Hopf, Frobenius and quadratic alternative algebras. These results allow us to justify from the point of view of the foundations of mathematics the uniqueness of these algebras, the matrix representation of the quaternions and exhibit a “ matrix ” representation of the octonions.

The work consists of three chapters. In the first chapter we provide some concepts and some results of real and topology algebras.

In chapter two, we prove that any commutative real algebra of divison of finite dimension has dimension less than or equal to two. We describe the algebra of the quaternions and display a matrix representation of this algebra. We study some results of the alternative algebras that allow us to prove that any real algebra $\mathcal{A} \neq 0$ associative, quadratic without divisors of zero of dimension greater than two is isomorphic to the algebra of the quaternions.

In the third chapter we study some results of quadratic alternative algebras, which allow us to describe the algebra of the octonions. We prove that all alternative real algebra, quadratic without divisors of zero and non-associative, is isomorphic to the algebra of the octonions. Finally we provide a “ matrix ” representation of the octonions.

Keywords:

- Álgebra without zero divisors.
- Alternative algebra.
- Quadratic algebra.

Índice general

Capítulo 1

Introducción

1.1. Álgebras reales

1.1.1 Definición. Se dice que un espacio vectorial V sobre $\mathbb{R}$ con una aplicación $\cdot : V \times V \to V$, $\cdot(x, y) = xy$ es un álgebra sobre $\mathbb{R}$ (o un $\mathbb{R}$-álgebra o álgebra real) si, y solo si,

$$(\alpha x + \beta y)z = \alpha(xz) + \beta(yz) \quad \text{y} \quad x(\alpha y + \beta z) = \alpha(xy) + \beta(xz)$$

para todo $\alpha, \beta \in \mathbb{R}$ y para todo $x, y, z \in V$.

Se dice que un $\mathbb{R}$-álgebra es asociativa si, y solo si, $x(yz) = (xy)z$ para todo $x, y, z \in V$.

Un $\mathbb{R}$-álgebra es llamada álgebra conmutativa si, y solo si, $xy = yx$ para todo $x, y \in V$. En otro caso, es llamada álgebra no conmutativa.

Un elemento $e \in V$ es llamado elemento identidad (o elemento unidad) de un álgebra si, y solo si, $ex = xe = x$ para todo $x \in V$.

Escribiremos $\mathcal{A} = (V, \cdot)$ para distinguir entre diferentes álgebras definidas sobre V.

1.1.2 Definición. Sea $\mathcal{A} = (V, \cdot)$ un $\mathbb{R}$-álgebra.

1. La dimensión del álgebra $\mathcal{A}$, se define como la dimensión de V.

2. Se dice que $\mathcal{A}$ es una potencia-asociativa si, y solo si, $x^m x^n = x^{m+n}$ para todo $x \in V$ y para todo $m \geq 1$, $n \geq 1$.

3. Se dice que un elemento x de $\mathcal{A} - \{0\}$ es un divisor de cero en $\mathcal{A}$ si, y solo si, existe un elemento $y \neq 0$ tal que $xy = 0$ o $yx = 0$.

Ejemplos.

1. Los cuerpos $\mathbb{R}$ y $\mathbb{C}$ son $\mathbb{R}$-álgebras asociativas y conmutativas de dimensiones 1 y 2 respectivamente, cada una con elemento identidad y sin divisores de cero.

2. El $\mathbb{R}$-espacio vectorial $\mathrm{Mat}(n, \mathbb{R})$ de todas las matrices reales $n \times n$, es un $\mathbb{R}$-álgebra asociativa con elemento identidad (matriz identidad) de dimensión n^2, con respecto a la multiplicación de matrices.

3. El $\mathbb{R}$-espacio vectorial $\mathrm{Mat}(n, \mathbb{C})$ de todas las matrices complejas $n \times n$, es un $\mathbb{R}$-álgebra asociativa de dimensión $2n^2$, con elemento identidad respecto a la multiplicación de matrices.
   Note que las álgebras $\mathrm{Mat}(n, \mathbb{R})$ y $\mathrm{Mat}(n, \mathbb{C})$ no son conmutativas cuando $n > 1$.

4. Dados dos vectores $a = (\alpha_1, \alpha_2, \alpha_3), b = (\beta_1, \beta_2, \beta_3) \in \mathbb{R}^3$, definimos el producto vectorial $\times : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3$ por

$$a \times b = (\alpha_2\beta_3 - \alpha_3\beta_2, \alpha_3\beta_1 - \alpha_1\beta_3, \alpha_1\beta_2 - \alpha_2\beta_1) \in \mathbb{R}^3.$$

   El espacio vectorial $\mathbb{R}^3$ con esta multiplicación es un $\mathbb{R}$-álgebra de dimensión 3, que es no asociativa y es anti-conmutativa ($a \times b = -b \times a$).

5. Sea V el $\mathbb{R}$-espacio vectorial de todas las matrices simétricas reales de orden $n \times n$ ($A^t = A$). Dadas las matrices $A, B \in V$, definimos $A \cdot B$ como

$$A \cdot B = \frac{1}{2}(AB + BA)$$

   Con esta multiplicación el $\mathbb{R}$-espacio vectorial V es un álgebra conmutativa que no es asociativa cuando $n > 1$.

1.1.3 Nota. Sea $V \neq 0$ un $\mathbb{R}$ espacio vectorial. Fijemos un elemento $e \in V - \{0\}$ y sea U cualquier espacio suplementario de $\mathbb{R}e$. Para $x = \alpha e + u, x' = \alpha' e + u' \in \mathbb{R}e \oplus U$ definimos la multiplicación $xx' = (\alpha\alpha')e + \alpha u' + \alpha' u$.

Dados $s, t \in \mathbb{R}$ y $x = \alpha e + u, y = \beta e + v, z = \gamma e + w \in V = \mathbb{R}e \oplus U$, se tiene

$$\begin{aligned}
\circ\ (sx + ty)z &= (s\alpha e + su + t\beta + tv)(\gamma e + w) \\
&= (\,(s\alpha + t\beta)e + su + tv\,)\,(\gamma e + w) \\
&= (s\alpha + t\beta)\gamma e + (s\alpha + t\beta)w + \gamma(su + tv) \\
&= s(\alpha\,\gamma e + \alpha w + \gamma u) + t(\beta\,\gamma e + \beta w + \gamma v) \\
&= s(xz) + t(yz)
\end{aligned}$$

Análogamente, $x(sy + tw) = s(xy) + y(xw)$.

Por otro lado,

$$\begin{aligned}
\circ\ (xy)z &= (\alpha\beta e + \alpha v + \beta u)(\gamma e + w) \\
&= (\alpha\beta\gamma)e + \alpha\beta w + \gamma(\alpha v + \beta u)
\end{aligned}$$

$$\begin{aligned}
\circ\ x(yz) &= (\alpha e + u)(\beta\gamma e + \beta w + \gamma v) \\
&= (\alpha\beta\gamma)e + \alpha(\beta w + \gamma v) + \beta\gamma u
\end{aligned}$$

Es decir, $x(yz) = (xy)z$.

Además, $xy = (\alpha\beta)e + \alpha v + \beta u = (\beta\alpha)e + \beta u + \alpha v = yx$.

En consecuencia $(V, \cdot)$ es un $\mathbb{R}$-álgebra conmutativa, asociativa, con elemento identidad e y tal que todo elemento de U es un divisor de cero.

1.1.4 Definición. Se dice que un subespacio real U de un $\mathbb{R}$-álgebra $\mathcal{A} = (V, \cdot)$ es un $\mathbb{R}$-subálgebra de $\mathcal{A}$ si, y solo si, $xy \in U$ para todo $x, y \in U$.

Ejemplo.- Sea el $\mathbb{R}$-espacio vectorial

$$U = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \ ;\ a, b \in \mathbb{R} \right\}.$$

Para $x = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}, y = \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \in U$, se tiene que

$$xy = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac - bd & -(bc + ad) \\ bc + ad & ac - bd \end{pmatrix} \in U.$$

Por tanto, U es una $\mathbb{R}$-subálgebra de $\mathrm{Mat}(2, \mathbb{R})$.

1.1.5 Definición. Sean $\mathcal{A} = (V, \cdot)$ y $\mathcal{B} = (W, \cdot)$ dos álgebras cualesquiera. Una aplicación $\mathbb{R}$-lineal $f : V \to W$ es un homomorfismo de $\mathbb{R}$-álgebras si, y solo si, $f(xy) = f(x)f(y)$ para todo $x, y \in V$.

Un homomorfismo de $\mathbb{R}$-álgebras que es inyectivo (respectivamente suryectivo, biyectivo) es llamado monomorfismo (respectivamente epimorfismo, isomorfismo) de álgebras. Si $V = W$, f es llamado un endomorfismo de álgebras.

Ejemplo.- Sea $f : \mathbb{C} \to \mathrm{Mat}(2, \mathbb{R})$ definida por $f(a+bi) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

Dados $x = a + bi, y = c + di \in \mathbb{C}$, se tiene

$$\begin{aligned} f(xy) &= f\left((ac-bd)+(ad+bc)i\right) \\ &= \begin{pmatrix} ac-bd & -(ad+bc) \\ ad+bc & ac-bd \end{pmatrix} \\ &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \\ &= f(x)f(y) \end{aligned}$$

Por ende, la aplicación f es un monomorfismo de álgebras.

1.1.6 Nota. Si $\mathcal{A}$ es un álgebra con elemento identidad e, entonces $f : \mathbb{R} \to \mathcal{A}$ definida por $f(\alpha) = \alpha e$ es un monomorfismo de álgebras. En particular toda álgebra real de dimensión uno con elemento identidad es isomorfa a $\mathbb{R}$.

1.1.7 Teorema. Si $\mathcal{A}$ es un álgebra de dimensión uno y su multiplicación no es la aplicación cero, $\mathcal{A}$ es isomorfa al álgebra $\mathbb{R}$.

Prueba. Según (1.1.6) bastará probar que $\mathcal{A}$ tiene elemento identidad. Es claro que $\mathcal{A} = \mathbb{R}a$ con $a \in \mathcal{A} - \{0\}$. Como la multiplicación no es la aplicación cero, existen $x, y \in \mathcal{A} - \{0\}$ tales que $xy \neq 0$. Es decir existen $\alpha, \beta \in \mathbb{R} - \{0\}$ tales que $(\alpha a)(\beta a) \neq 0$, por ende $a^2 \neq 0$. Como también $\mathcal{A} = \mathbb{R}a^2$ y $a \in \mathcal{A}$, existe $t \in \mathbb{R}$ tal que $a = ta^2$. Por lo tanto, $e = ta$ es un elemento identidad de $\mathcal{A}$.$\blacksquare$

1.1.8 Definición. Un álgebra $\mathcal{A} \neq 0$ es un álgebra de división si, y solo si, para todo $a, b \in V$ con $a \neq 0$, las ecuaciones $ax = b$ y $ya = b$ tienen soluciones únicas en $\mathcal{A}$.

Ejemplos

1. Los cuerpos $\mathbb{R}$ y $\mathbb{C}$ son álgebras de división asociativas y conmutativas, de dimensiones 1 y 2 respectivamente.

2. Las álgebras de matrices $\mathrm{Mat}(n, \mathbb{R})$ y $\mathrm{Mat}(n, \mathbb{C})$ no son álgebras de división cuando $n > 1$.

1.1.9 Teorema. Sea $* : G \times G \to G$ una operación binaria tal que $a*(b*c) = (a*b)*c$ para todo $a, b, c \in G$. $(G, *)$ es un grupo si, y solo si,

1. Existe $e_d \in G$ tal que $x * e_d = x$ para todo $x \in G$

2. Para todo $a \in G$, existe $a_d \in G$ tal que $a * a_d = e_d$.■

Prueba. Ver [4], pág. 44.■

1.1.10 Lema. Si $\mathcal{A}$ es un álgebra de división asociativa, entonces $G = \mathcal{A} - \{0\}$ es un grupo con respecto a la multiplicación en $\mathcal{A}$. El elemento neutro de G es el elemento identidad de $\mathcal{A}$.

Prueba. Como $\mathcal{A}$ es un álgebra de división asociativa, para todo $a, b \in G$ las ecuaciones

$$ax = b \tag{1.1}$$

$$ya = b \tag{1.2}$$

tienen solución única en G para todo $a, b \in G$.
Por (1.1.9) para que G sea grupo, bastará probar que

a) Existe un $e_G \in G$ tal que $g.e_G = g$ para todo $g \in G$

b) Dado $g \in G$, existe $\hat{g} \in G$ tal que $g.\hat{g} = e_G$

Dado $a \in G$, por (1.1) existe $x_a \in G$ tal que $a.x_a = a$. Por otro lado, dados $a, g \in G$ arbitrarios, existen $n, m \in G$ tales que $a.n = g$ y $m.a = g$ (ver 1.1 y 1.2).
Ahora, $g.x_a = (m.a).x_a = m.(a.x_a) = m.a = g$. Es decir, existe $e_G = x_a \in G$ tal que $g.e_G = g$ para toda $g \in G$.
Sea $g \in G$ cualesquiera. Como $e_G \in G$, la ecuación (1.1) garantiza que existe $\hat{g} \in G$ tal que $g.\hat{g} = e_G$.
En consecuencia, $(G, \cdot)$ es un grupo y como en un grupo la unidad es única, e_G es la identidad de $\mathcal{A}$.■

1.1.11 Teorema. Si $\mathcal{A}$ es un álgebra de división, $\mathcal{A}$ no tiene divisores de cero.

Prueba. Supongamos que existe $a \in \mathcal{A} - \{0\}$ divisor de cero en $\mathcal{A}$.
Como $a \neq 0$ y $\mathcal{A}$ es un álgebra de división, las ecuaciones $ax = 0$ y $ya = 0$ tienen soluciones únicas.
Como $a \in \mathcal{A} - \{0\}$ es divisor de cero en $\mathcal{A}$, existe $b \neq 0$ tal que $ab = 0$ o $ba = 0$.
Como las soluciones de $ax = 0$ y $ya = 0$ son únicas, se tiene que $b = 0$ (una contradición). En consecuencia, $\mathcal{A}$ no tiene divisores de cero.$\blacksquare$

1.1.12 Teorema. Si $\mathcal{A}$ es un álgebra de dimensión finita y no tiene divisores de cero, entonces $\mathcal{A}$ es un álgebra de división.

Prueba. Sea $a \in \mathcal{A} - \{0\}$. Es claro que la aplicación $\varphi : \mathcal{A} \to \mathcal{A}$ definida por $\varphi(x) = ax$ es lineal. Si $\varphi(x) = 0$, se tiene $ax = 0$ y como $\mathcal{A}$ no tiene divisores de cero, $x = 0$.
Como $\mathcal{A}$ es de dimensión finita finita, se concluye que φ es sobreyectiva. Ahora, como φ es biyección, $ax = b$ tiene solución única. Analogamente, si definimos $\xi : \mathcal{A} \to \mathcal{A}$ por $\xi(y) = ya$, la ecuación $ya = b$ tiene solución única.$\blacksquare$

1.2. Algunos conceptos topológicos

1.2.1 Definición.

1. Una aplicación $f : X \to Y$ entre espacios topológicos es un homeomorfismo local de $x \in X$ si, y solo si, existe una vecindad abierta U de x cuya imagen $f(U)$ es un abierto en Y y la aplicación $f|_U : U \to f(U)$ es un homeomorfismo.

2. Una aplicación $p : X \to Y$ entre espacios topológicos es llamada un recubrimiento si, y solo si, p es sobreyectiva y para todo punto $y \in Y$ existe una vecindad abierta W de y tal que $p^{-1}(W) = \bigcup_{j \in J} U_j$ para alguna familia $\{U_j; j \in J\}$ de abiertos en X tales que $U_j \cap U_k = \phi$ para $j \neq k$ y $p|_{U_j} : U_j \to W$ es un homeomorfismo para cada $j \in J$.

3. Un recubrimiento $p : X \to Y$ es llamado conexo si, y solo si, X es un espacio conexo.

4. Se dice que $p : X \to Y$ es un recubrimiento de grado $k, k \in \mathbb{Z}^+$ si, y solo si, para todo $y \in Y$, $p^{-1}(y)$ tiene exactamente k elementos diferentes.

1.2.2 Definición. Sea V un espacio vectorial real(no necesariamente finito dimensional). Una aplicación $\| \| : V \to \mathbb{R}$, $x \mapsto \|x\|$ es una norma en V si, y solo si, para todo $x, y \in V$ y para todo $\alpha \in \mathbb{R}$ se verifica las siguientes condiciones

1. $\|x\| > 0$, para $x \neq 0$
2. $\|\alpha x\| \leq |\alpha| \, \|x\|$
3. $\|x + y\| \leq \|x\| + \|y\|$

Un espacio vectorial V con una norma $\| \|$ definida en V, es llamado espacio normado y se denota por $(V, \| \|)$.

1.2.3 Nota. Sea V un $\mathbb{R}$- espacio vectorial

1. Una norma $\| \| : V \to \mathbb{R}, x \mapsto \|x\|$ es una aplicación continua.
2. Una norma $\| \|$ en V induce una métrica $d : V \times V \to \mathbb{R}$ en V definida por $d(x, y) = \|x - y\|$.
3. Las aplicaciones $V \times V \to V, (x, y) \mapsto x + y$ y $\mathbb{R} \times V \to V, (\alpha, x) \mapsto \alpha x$ son continuas.
4. En todo espacio normado $(V, \| \cdot \|)$ de dimensión finita la esfera unitaria $\mathbb{S} = \{x \in V; \|x\| = 1\}$ es un conjunto compacto.
5. Todo espacio vectorial euclideano V con producto escalar $\langle x, y \rangle$ tiene norma $\| \| : V \to \mathbb{R}$ definida por $\|x\| = \sqrt{\langle x, x \rangle}$.

1.2.4 Teorema. Si V es un $\mathbb{R}$-espacio vectorial normado y $\dim V \geq 3$, entonces todo recubrimiento conexo $p : X \to V \setminus \{0\}$ es de grado uno.

Prueba. Si $\dim V \geq 3$ es finita, podemos considerar V como un $\mathbb{R}^n$ con $n \geq 3$. Dada la esfera unitaria $S^{n-1} = \{x \in \mathbb{R}^n; \|x\| = 1\}$, es claro que la aplicación $f : \mathbb{R}^n \setminus \{0\} \to \mathbb{R}^+ \times S^{n-1}$ definida por $f(x) = \left(\|x\|, \dfrac{x}{\|x\|} \right)$ es un homeomorfismo

($f^{-1} : \mathbb{R}^+ \times S^{n-1} \to \mathbb{R}^n \setminus \{0\}$, $f^{-1}(\alpha, x) = \alpha x$).
Como S^{n-1} es simplemente conexo, se concluye que $\mathbb{R}^n \setminus \{0\}$ es simplemente conexo (ver [7], pág. 380).

Para el caso V infinito dimensional, consideremos γ un camino cerrado en $V \setminus \{0\}$. Ahora subdiviremos γ en un número finito de partes cada una en una bola en $V \setminus \{0\}$. Como las bolas son convexas, estos caminos parciales se pueden deformar dentro de sus bolas en segmentos de línea. Obteniendo de este modo una deformación de γ en $V \setminus \{0\}$ en una trayectoría poligonal cerrada en $V \setminus \{0\}$. Esta poligonal se encuentra en algún subespacio de dimensión finita $\mathbb{R}^n$ ($n \geq 3$) de V y en consecuencia puede deformarse continuamente a un punto en $\mathbb{R}^n \setminus \{0\}$.

Ahora consideremos un recubrimiento conexo arbitrario $p : X \to V \setminus \{0\}$. Sean $x_1, x_2 \in X$ tales que $p(x_1) = p(x_2)$ y consideremos un camino $\tilde{\gamma}$ en X de x_1 a x_2. Es claro que $\gamma = p \circ \tilde{\gamma}$ es un camino cerrado en $V \setminus \{0\}$. Como $V \setminus \{0\}$ es simplemente conexo, γ es contractible en $V \setminus \{0\}$ a su punto inicial $p(x_1)$ por deformación a través de una familia continua de caminos γ_s, $0 \leq s \leq 1$. Como $p : X \to V \setminus \{0\}$ es un recubrimiento, cada camino γ_s tiene un único levantamiento $\tilde{\gamma}_s$ sobre γ_s con punto inicial x_1 (ver [7], pág. 388). Entonces $\tilde{\gamma}_s$, $0 \leq s \leq 1$ es una familia de caminos continuos en X con $\tilde{\gamma}_0 = \tilde{\gamma}$ y $\tilde{\gamma}_1$ el camino consistente del punto x_1. Como todos los caminos tienen el mismo punto final (ver [7], pág. 391), se concluye que x_2 es el punto final de $\tilde{\gamma}_0$ e igual al punto final de $\tilde{\gamma}_1$ que es x_1. Por lo tanto, todo conjunto $p^{-1}(y)$ con $y \in V \setminus \{0\}$ tiene un único elemento.$\blacksquare$

Capítulo 2

Los números cuaterniones

2.1. El teorema de Hopf

En esta sección estudiaremos las álgebras reales de dimensión finita, conmutativas y de división; no necesariamente asociativas.

2.1.1 Lema. Si $\mathcal{A} = (V, \cdot)$ es un álgebra real de dimensión finita y $\| \ \|$ es una norma en V, entonces

1) La multiplicación $\mathcal{A} \times \mathcal{A} \to \mathcal{A}, (x, y) \mapsto xy$ es una aplicación continua.

2) Existe un $r \geq 0$ tal que $\|xy\| \leq r\|x\| \, \|y\|$ para todo $x, y \in \mathcal{A}$.

3) Si $\mathcal{A}$ no tiene divisores de cero, existe $\xi > 0$ tal que $\xi \, \|x\| \, \|y\| \leq \|xy\|$ para todo $x, y \in \mathcal{A}$.

Prueba.

1) Sea $v_1, \ldots, v_n$ una base de V. Dados $x, y \in V$, existen $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{R}$ tales que $x = a_1v_1 + \cdots + a_nv_n$ y $y = b_1v_1 + \cdots + b_nv_n$. Como la aplicación $\mathcal{A} \to \mathbb{R}^n$, $x \mapsto (a_1, \ldots, a_n)$ es continua, entonces cada función $f_k : \mathcal{A} \to \mathbb{R}$, $f_k(x) = a_k$ es continua. Dado que xy es una suma de términos de la forma $a_ib_jv_iv_j$, se tiene que xy es continua.

2) Como $\|\alpha x\| = |\alpha|\|x\|$, bastará probar que existe $r > 0$ tal que $\|xy\| \leq r$ para todo $x, y \in \mathbb{S} = \{u \in V; \|u\| = 1\}$. Es claro que la aplicación

$\mathbb{S} \times \mathbb{S} \to \mathbb{R}, (x,y) \mapsto \|xy\|$ es continua y como $\mathbb{S} \times \mathbb{S}$ es compacto, existe $r \geq 0$ tal que $\|xy\| \leq r$ para todo $x, y \in \mathbb{S}$.

3) Analogamente existe $\xi \geq 0$ tal que $\xi \leq \|xy\|$ para todo $x, y \in \mathbb{S}$. Como $\mathcal{A}$ no tiene divisores de cero y $x, y \in \mathbb{S} \subset \mathcal{A} - \{0\}$, $xy \neq 0$. Por ende, $\xi > 0$.■

2.1.2 Teorema. Si $\mathcal{A}$ es un álgebra normada de dimensión finita y no tiene divisores de cero, entonces el conjunto $F = \{x^2; x \in \mathcal{A} - \{0\}\}$ es cerrado en $\mathcal{A} - \{0\}$.

Prueba. Sea (x_n^2) una sucesión en F tal que $\lim\limits_{n\to+\infty} x_n^2 = a$ con $a \in \mathcal{A} - \{0\}$. Probaremos que existe $b \in \mathcal{A} - \{0\}$ tal que $b^2 = a$. Note que (x_n^2) es acotada, pues ella es convergente. Por (3) de (2.1.1), existe $\rho > 0$ tal que $\|x_n^2\| \geq \rho \|x_n\|^2$ para todo $n \in \mathbb{N}$. Es decir, $(x_n) \subset \mathcal{A} - \{0\}$ es acotada. Por el teorema de Bolzano-Weierstrass existe una subsucesión (y_n) de (x_n) tal que $\lim\limits_{n\to+\infty} y_n = b$. Ahora por (1) de (2.1.1) se tiene $b^2 = \lim\limits_{n\to+\infty} y_n^2 = a$.■

Note que para toda $\mathbb{R}$-álgebra la aplicación cuadrática $\mathcal{A} \to \mathcal{A}, x \mapsto x^2$ esta bien definida. Denotemos $\mathcal{A} - \{0\}$ por $\mathcal{A}^*$. Si $\mathcal{A}$ no tiene divisores de cero, es claro que $x^2 \in \mathcal{A}^*$ para todo $x \in \mathcal{A}^*$. En consecuencia, la aplicación $q : \mathcal{A}^* \to \mathcal{A}^*$ dada por $q(x) = x^2$ esta bien definida.

2.1.3 Teorema. Si $\mathcal{A}$ es una $\mathbb{R}$-álgebra conmutativa y sin divisores de cero, entonces todo punto de la imagen $q(\mathcal{A}^*)$ tiene exactamente dos imagenes inversas en $\mathcal{A}^*$.

Prueba. Dado $w \in q(\mathcal{A}^*)$, existe $a \in \mathcal{A}^*$ tal que $w = a^2$. Es claro que $-a \in \mathcal{A}^*$ y $(-a)^2 = a^2 = w$. Verifiquemos que a y $-a$ son las únicas imagenes inversas de w. Supongamos que existe $b \in \mathcal{A}^*$ tal que $b^2 = w$. Se tiene,

$$\begin{aligned} a^2 = w = b^2 \quad &\Leftrightarrow \quad a^2 - b^2 = 0 \\ &\Leftrightarrow \quad (a-b)(a+b) = 0 \\ &\Leftrightarrow \quad b = a \vee b = -a \end{aligned}$$

Como $a \neq -a$, entonces $q^{-1}(w)$ tiene exactamente dos imagenes inversas.■

2.1.4 Teorema. Sea $\mathcal{A} = (V, \cdot)$ un álgebra real conmutativa sin divisores de cero de dimensión finita tal que

i) Existe una norma sobre V tal que la aplicación cuadrática $q : \mathcal{A}^* \to \mathcal{A}^*$, dada por $q(x) = x^2$ es un homeomorfismo local en todos los puntos de $\mathcal{A}^*$.

ii) Todo elemento de $\mathcal{A}$ es un cuadrado.

Entonces dim$\mathcal{A} = 2$.

Prueba. Note que dim$\mathcal{A} \geq 2$, caso contrario por el teorema (1.1.7) $\mathcal{A}$ sería isomorfa a $\mathbb{R}$, pero esto no es posible pues no existe $r \in \mathbb{R}$ tal que $r^2 = -1$. En consecuencia, $\mathcal{A}^*$ es conexo. Dado $a \in \mathcal{A}^*$, por (ii) existe $b \in \mathcal{A}^*$ tal que $b^2 = a$. Es decir, la aplicación cuadrática q es sobreyectiva.

`Afirmación`.- La aplicación $q : \mathcal{A}^* \to \mathcal{A}^*$ es un recubrimiento conexo de grado 2. Sea $w \in \mathcal{A}^*$ fijo pero arbitrario. Por (2.1.3), se tiene que $q^{-1}(w) = \{a, -a\}$ para algún $a \in \mathcal{A}^*$. Por (i) existen vecindades abiertas U, V de a y $-a$ respectivamente, tales que $q(U)$, $q(V)$ son abiertos y $q : U \to q(U)$, $q : V \to q(V)$ son homeomorfismos. Como $\mathcal{A}^*$ es un espacio de Hausdorff, podemos asumir que $U \cap V = \phi$. Ahora definamos $W := q(U) \cap q(V)$, $U_1 := q^{-1}(W) \cap U$, $V_1 := q^{-1}(W) \cap V$. Es claro que W, U_1, V_1 son vecindades abiertas y no vacías de w, a y $-a$ respectivamente, $U_1 \cap V_1 = \phi$ y que las aplicaciones $q : U \to W$, $q : V \to W$ son homeomorfismos. Como $q^{-1}(W) = U_1 \cup V_1$, se tiene que q es un recubrimiento conexo de grado 2. Finalmente, de (1.2.4) se concluye que dim$\mathcal{A} = 2$.$\blacksquare$

Ahora presentaremos algunos conceptos de cálculo diferencial sobre espacios de Banach.

2.1.5 Definición. Sea $\mathcal{A} = (V, \cdot)$ un $\mathbb{R}$-álgebra de división normada de dimensión finita. Una función $f : V \to V$ es diferenciable en el punto $a \in V$, si y solo si, existe una transformación $\mathbb{R}$-lineal $f'_a : V \to V$ tal que

$$\lim_{h \to 0} \frac{\|f(a+h) - f(a) - f'_a(h)\|}{\|h\|} = 0.$$

La aplicación f'_a si existe es única y es llamada la derivada de f en el punto a. Cada elemento $a \in \mathcal{A}$ define, multiplicando a derecha e izquierda las aplicaciones lineales $L_a : \mathcal{A} \to \mathcal{A}, L_a(x) = ax$ y $R_a : \mathcal{A} \to \mathcal{A}, R_a(x) = xa$.

2.1.6 Teorema. Si $\mathcal{A} = (V, \cdot)$ es un $\mathbb{R}$-álgebra de división de dimensión finita, la aplicación cuadrática $q : \mathcal{A} \to \mathcal{A}, q(x) = x^2$ es diferenciable en a para todo punto $a \in \mathcal{A}$ y $q'_a = L_a + R_a$. Si $\mathcal{A}$ es conmutativa, entonces q'_a es biyectiva para todo $a \in \mathcal{A}^*$.

Prueba. Dado $h \in \mathcal{A}$ con $h \neq 0$, se tiene

$$q(a+h) = (a+h)^2 = a^2 + ah + ha + h^2 = q(a) + (L_a + R_a)(h) + h^2.$$

Por (2) de (2.1.1) existe $r \geq 0$ tal que $\|h^2\| \leq r\|h\|^2$. En consecuencia

$$\frac{\|q(a+h) - q(a) - (L_a + R_a)(h)\|}{\|h\|} = \frac{\|h^2\|}{\|h\|} \leq r\|h\|$$

que tiende a cero cuando h tiende a cero. Por tanto, $q'_a = L_a + R_a$ para todo $a \in \mathcal{A}$. Es decir, $q'_a(x) = ax + xa$, $x \in \mathcal{A}$.
Si $\mathcal{A}$ es conmutativa, $L_a = R_a$, en consecuencia $q'_a(x) = 2ax$, $x \in \mathcal{A}$. Para $a \in \mathcal{A}$ con $a \neq 0$, q'_a es inyectiva, pues $\mathcal{A}$ no tiene divisores de cero. Como la dimensión de $\mathcal{A}$ es finita, q'_a es biyectiva.■

Dado el espacio vectorial V sobre $\mathbb{R}$, denotemos por $\mathcal{L}_{\mathbb{R}}(V)$ al espacio vectorial de las transformaciones $\mathbb{R}$-lineales de V en V. Una aplicación $f : V \to V$ diferenciable en V induce una aplicación $f' : V \to \mathcal{L}_{\mathbb{R}}(V)$, $v \mapsto f'(v)$.

2.1.7 Definición. Se dice que una aplicación $f : V \to V$ diferenciable en V es continuamente diferenciable si, y solo si, f' es continua.

2.1.8 Teorema. Sea $f : V \to V$ continuamente diferenciable. Si $v \in V$ es tal que la derivada $f'(v) : V \to V$ es biyectiva, entonces f es un homeomorfismo local de v.■

2.1.9 Teorema. Sea $\mathcal{A} = (V, \cdot)$ un $\mathbb{R}$-álgebra de división de dimensión finita. Si $\mathcal{A}$ es conmutativa, la aplicación $q : \mathcal{A}^* \to \mathcal{A}^*, q(x) = x^2$ es un homeomorfismo local.

Prueba. Por (2.1.6), para cada $a \in \mathcal{A}^*$, su derivada $q'(a)$ es biyectiva. Además la aplicación $q' : \mathcal{A}^* \to Hom_{\mathbb{R}}(\mathcal{A}, \mathcal{A}), a \mapsto 2L_a$ es continua, es decir, q es continuamente diferenciable. Entonces por el teorema (2.1.8), se concluye que la aplicación cuadrática $q : \mathcal{A}^* \to \mathcal{A}^*, q(x) = x^2$ es un homeomorfismo local.■

2.1.10 Teorema (De Hopf)**.** La dimensión de toda $\mathbb{R}$-álgebra normada conmutativa de división y de dimensión finita es como máximo 2.

Prueba. Por (2.1.9), se cumple la condición (i) de (2.1.4). Sea $n = \dim\mathcal{A}$. Si $n \geq 2$, entonces $\mathcal{A}^*$ es conexo. Como $q : \mathcal{A}^* \to \mathcal{A}^*, q(x) = x^2$ es un homeomorfismo local, la aplicación q es abierta; por ende $q(\mathcal{A}^*)$ es un subconjunto abierto y no vacío de $\mathcal{A}^*$. Ahora por (2.1.2), la imagen $q(\mathcal{A}^*)$ es un subconjunto cerrado de $\mathcal{A}^*$. Como $\mathcal{A}^*$ es conexo, se tiene que $q(\mathcal{A}^*) = \mathcal{A}^*$. Es decir se cumple la parte (ii) de (2.1.4). Por lo tanto, $n = 2$.■

2.2. El álgebra de los cuaterniones

Consideremos el $\mathbb{R}$-espacio vectorial $\mathbb{R}^4 = \{(x_1, x_2, x_3, x_4); x_i \in \mathbb{R}, 1 \leq i \leq 4\}$ y denotemos la base canónica

$$e_1 = (1,0,0,0),\ e_2 = (0,1,0,0),\ e_3 = (0,0,1,0),\ e_4 = (0,0,0,1)$$

de $\mathbb{R}^4$ por $e_1 = e, e_2 = i, e_3 = j, e_4 = k$.

2.2.1 Definición. Dados $x = (x_1, x_2, x_3, x_4), y = (y_1, y_2, y_3, y_4) \in \mathbb{R}^4$, definimos el producto xy como

$$xy = (x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4\ ,\ x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3\ ,\ x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2\ ,\ x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1)$$

El $\mathbb{R}$-espacio vectorial $\mathbb{R}^4$ con este producto es un $\mathbb{R}$-álgebra de dimensión cuatro, llamada `álgebra de los cuaterniones` y se denota por $\mathbb{H}$. Los elmentos de $\mathbb{H}$ son llamados `números cuaterniones` o `cuaternios`.

2.2.2 Nota. De la definicón (2.2.1) se tiene

1. Dado $q = (q_1, q_2, q_3, q_4) \in \mathbb{H}$, $qe = (q_1, q_2, q_3, q_4) = eq$. Es decir, e es el elemento identidad de $\mathbb{H}$.

2. Como $e_2e_3 = (0,0,0,1) \neq (0,0,0,-1) = e_3e_2$ el álgebra de los cuaterniones $\mathbb{H}$ no es conmutativa.

3. $$\begin{array}{ll} (e_2e_3)e_4 = e_4e_4 = -e_1 & ;\quad e_2(e_3e_4) = e_2e_2 = -e_1 \\ (e_2e_4)e_3 = (-e_3)e_3 = e_1 & ;\quad e_2(e_4e_3) = e_2(-e_2) = e_1 \\ (e_3e_2)e_4 = (-e_4)e_4 = e_1 & ;\quad e_3(e_2e_4) = e_3(-e_3) = e_1 \\ (e_4e_2)e_4 = e_3e_4 = e_2 & ;\quad e_4(e_2e_4) = e_4(-e_3) = -(-e_2) \end{array}$$

   de este modo podemos verificar que las 27 igualdades $(e_\lambda e_\mu)e_\nu = e_\lambda(e_\mu e_\nu)$ con $2 \leq \lambda, \mu, \nu \leq 4$ son válidas, en consecuencia $\mathbb{H}$ es un álgebra asociativa.

4. Si denotamos e_1, e_2, e_3, e_4 por e, i, j, k respectivamente, obtenemos

$$i^2 = j^2 = k^2 = ijk = -e,\ ij = -ji = k.$$

5. Los nueve productos $e_\mu e_\lambda$ con $2 \leq \mu, \lambda \leq 4$ los podemos expresar en la siguiente tabla de multiplicación

$\cdot$	e_2	e_3	e_4
e_2	$-e_1$	e_4	$-e_3$
e_3	$-e_4$	$-e_1$	e_2
e_4	e_3	$-e_2$	$-e_1$

2.2.3 Teorema. El conjunto $\mathcal{C}$ de todas las matrices reales 2×2, $\begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix}$ con $\alpha, \beta \in \mathbb{R}$ es un $\mathbb{R}$-subálgebra de $\mathrm{Mat}(2; \mathbb{R})$ y la aplicación $\alpha + \beta i \longmapsto \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix}$ es un isomorfismo de $\mathbb{R}$-álgebras $\mathbb{C} \to \mathcal{C}$.■

2.2.4 Teorema. El conjunto $\mathcal{H} = \left\{ \begin{pmatrix} w & -z \\ \overline{z} & \overline{w} \end{pmatrix} ; z, w \in \mathbb{C} \right\}$ es un $\mathbb{R}$-subálgebra de $\mathrm{Mat}(2, \mathbb{C})$, con elemento unidad $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Toda matriz $A = \begin{pmatrix} w & -z \\ \overline{z} & \overline{w} \end{pmatrix} \in \mathcal{H}$ satisface sobre $\mathbb{R}$, la ecuación cuadrática

$$A^2 - (\mathrm{traza}A)A + (\det A)E = 0 \tag{2.1}$$

donde $\mathrm{traza}A = 2\mathrm{Re}\, w$ y $\det A = \|z\|^2 + \|w\|^2$. Además, $\mathcal{H}$ es un álgebra de división asociativa de dimensión 4.

Prueba. Es claro que $\mathcal{H}$ es un $\mathbb{R}$-subespacio vectorial de dimensión cuatro del espacio $\mathrm{Mat}(2; \mathbb{C})$, que es cerrado bajo la multiplicación de matrices. Por cálculo directo se puede verificar que $A^2 - (\mathrm{traza}A)A + (\det A)E = 0$.
Como $\mathrm{Mat}(2, \mathbb{C})$ es un álgebra asociativa, $\mathcal{H}$ es un $\mathbb{R}$-subálgebra asociativa.
Si $A, B \in \mathcal{H}$ son tales que $AB = 0$, entonves $\det A \det B = 0$. Luego, $\det A = 0$ o $\det B = 0$. Como $A, B \in \mathcal{H}$, se tiene que

$$\|z\|^2 + \|w\|^2 = \det A = 0 \quad \text{o} \quad \|z_1\|^2 + \|w_1\|^2 = \det B = 0.$$

En consecuencia, $A = 0$ o $B = 0$. Por (1.1.12), $\mathcal{H}$ es un álgebra de división.■

2.2.5 Teorema. La aplicación $F : \mathbb{H} \to \mathcal{H}$ definida por $F((\alpha,\beta,\gamma,\delta)) = \begin{pmatrix} \alpha+\beta i & -\gamma-\delta i \\ \gamma-\delta i & \alpha-\beta i \end{pmatrix}$, es un isomorfismo de $\mathbb{R}$-álgebras tal que $F(e_1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} := E$, $F(e_2) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} := I$, $F(e_3) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} := J$ y $F(e_4) = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} := K$.

Prueba. Es claro que F es $\mathbb{R}$-lineal y biyectiva.
Las matrices E, I, J, K verifican las relaciones

$$I^2 = J^2 = K^2 = -E,\ IJ = -JI = K,\ KI = -IK = J,\ JK = -KJ = I.$$

Es decir, las matrices E, I, J, K satisfacen las mismas relaciones de multiplicación que e_1, e_2, e_3, e_4.
Por otro lado, se tiene
$F(e_2)F(e_3) = IJ = K = F(e_4) = F(e_2\, e_3)\,,$
$F(e_2)F(e_4) = IK = -J = F(-e_3) = F(e_2\, e_4)\,,$
$F(e_4)F(e_3) = KJ = -I = F(-e_2) = F(e_4\, e_3)$. En esta forma podemos verificar que

$$F(e_i\, e_j) = F(e_i)F(e_j) \quad \text{para} \quad j = 1,2,3,4.$$

Por lo tanto, F es un isomorfismo de $\mathbb{R}$-álgebras.■

2.2.6 Corolario. El álgebra $\mathbb{H}$ es un $\mathbb{R}$-álgebra de división asociativa de dimensión cuatro.■

2.2.7 Definición. Dada la base estandar e, i, j, k de $\mathbb{H}$, el espacio imaginario de $\mathbb{H}$ denotado por $\mathrm{Im}\mathbb{H}$ se define como $\mathrm{Im}\mathbb{H} = \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$. Los elementos de $\mathrm{Im}\mathbb{H}$ son llamados imaginarios de los cuaternios.

Es claro que $\mathbb{H} = \mathbb{R}e \oplus \mathrm{Im}\mathbb{H}$. Por otro lado, dado $x = \alpha e + \beta i + \gamma j + \delta k \in \mathbb{H}$, el teorema (2.2.4) garantiza que

$$x^2 = 2\alpha x - \left(\alpha^2 + \beta^2 + \gamma^2 + \delta^2\right) e \tag{2.2}$$

Note que $x \in \mathrm{Im}\mathbb{H}$ si, y solo si, $\alpha = 0$. Ahora de la ecuación (2.2), se concluye que $x \in \mathrm{Im}\mathbb{H}$ si, y solo si, $x^2 \in \mathbb{R}e$ con $x \in \mathbb{R}e - \{0\}$. Esto nos permite escribir

$$\mathrm{Im}\mathbb{H} = \left\{x \in \mathbb{H}; x^2 \in \mathbb{R}e, x \notin \mathbb{R}e - \{0\}\right\}.$$

2.2.8 Nota. Observe que

1. Si $u = \beta i + \gamma j + \delta k \in \mathrm{Im}\mathbb{H}$, entonces $u^2 = -(\beta^2 + \gamma^2 + \delta^2)e$ con $\beta^2 + \gamma^2 + \delta^2 \geq 0$. Por ende, el espacio $\mathrm{Im}\mathbb{H}$ no es un $\mathbb{R}$-subálgebra de $\mathbb{H}$.

2. Como $\mathbb{H} = \mathbb{R}e \oplus \mathrm{Im}\mathbb{H}$, para todo $x \in \mathbb{H}$ existen $\alpha \in \mathbb{R}$ y $u \in \mathrm{Im}\mathbb{H}$ únicos tales que $x = \alpha e + u$.

3. Un producto interno en un espacio vectorial real V es una forma bilineal $\langle\, , \rangle : V \times V \to \mathbb{R}$ que tiene las siguientes propiedades

   a) Simetría: $\langle x, y\rangle = \langle y, x\rangle$.

   b) Definida positiva: $\langle x, x\rangle \geq 0$, y $\langle x, x\rangle = 0$ solo para el vector $x = 0$.

   Un espacio vectorial de dimensión finita en el cual está definido un producto interno es llamado llamado espacio euclideano.
   El número real $|x| := \sqrt{\langle x, x\rangle} \geq 0$ es llamado norma del vector x. Dos vectores $x, y \in V$ son ortogonales si, y solo si, $\langle x, y\rangle = 0$.

Ahora introduciremos un producto interno en el álgebra de cuaterniones, compatible con la multiplicación en $\mathbb{H}$.

2.2.9 Definición.

1. La aplicación $\langle\, , \rangle : \mathbb{H} \times \mathbb{H} \to \mathbb{R}$ definida por $\langle x, y\rangle = \alpha\alpha_1 + \beta\beta_1 + \gamma\gamma_1 + \delta\delta_1$ donde $x = \alpha e + \beta i + \gamma j + \delta k$ e $y = \alpha_1 e + \beta_1 i + \gamma_1 j + \delta_1 k$ es un producto interno en $\mathbb{H}$ llamado producto interno canónico.

2. Por analogía con la conjugación en $\mathbb{C}$, definimos la $\mathbb{R}$-conjugación lineal $^{-} : \mathbb{H} \to \mathbb{H}$ como $\overline{x} = \alpha e - u$ donde $x = \alpha e + u$.
   Es decir, si $x = (\alpha, \beta, \gamma, \delta) \in \mathbb{H}$, el conjugado de x es $\overline{x} = (\alpha, -\beta, -\gamma, -\delta)$.

3. Se define la forma $\mathbb{R}$-lineal $\mathrm{Re} : \mathbb{H} \to \mathbb{R}$ por $\mathrm{Re}(x) = \alpha$, donde $x = \alpha e + u$ con $\alpha \in \mathbb{R}$, $u \in \mathbb{H}$.
   Es decir, dado $x = (\alpha, \beta, \gamma, \delta) \in \mathbb{H}$ el real de x es $\mathrm{Re}(x) = \alpha$.

2.2.10 Observación. Ahora presentaremos algunas propiedades de los cuaternios.

1. Si $x = \alpha e + \beta i + \gamma j + \delta k \in \mathbb{H}$, se tiene $\langle x, x\rangle = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$. Por ende, $|x|^2 = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$.

2. $\forall\, x \in \mathbb{H} : |\,\overline{x}\,| = |x|,\ \overline{\overline{x}} = x$.

   $$\begin{aligned} x \in \mathrm{Im}\mathbb{H} &\Leftrightarrow x = \beta i + \gamma j + \delta k \\ &\Leftrightarrow \overline{x} = -\beta i - \gamma j - \delta k \\ &\Leftrightarrow \overline{x} = -(\beta i + \gamma j + \delta k) = -x \end{aligned}$$

   $\mathrm{Im}\mathbb{H} = \{x \in \mathbb{H}; \overline{x} = -x\}$

   $$\begin{aligned} x \in \mathrm{Re}\mathbb{H} &\Leftrightarrow \mathrm{Re}(x)e = \overline{x} \\ &\Leftrightarrow (\alpha, 0, 0, 0) = (\alpha, -\beta, -\gamma, -\delta) \\ &\Leftrightarrow x = (\alpha, 0, 0, 0) = \overline{x} \end{aligned}$$

   $\mathrm{Re}\mathbb{H} = \{x \in \mathbb{H}; \overline{x} = x\}$.

3. $\mathrm{Re}(e) = 1$, $\mathrm{Nuc}\,(\mathrm{Re}) = \mathrm{Im}\mathbb{H}$

   $\forall\, x \in \mathbb{H} : \mathrm{Re}(\overline{x}) = \mathrm{Re}(x),\ x + \overline{x} = 2\mathrm{Re}(x)e,\ x^2 = 2\mathrm{Re}(x)x - |x|^2 e.$

4. Dado $x = \alpha e + u$, se tiene $x\,\overline{x} = (\alpha e + u)(\alpha e - u) = \alpha^2 e - u^2 = \overline{x}\,x$. Note que $u^2 = (\beta i + \gamma j + \delta k)(\beta i + \gamma j + \delta k) = \beta^2 i^2 + \beta\gamma ij + \beta\delta ik + \gamma\beta ji + \gamma^2 j^2 + \gamma\delta jk + \delta\beta ki + \delta\gamma kj + \delta^2 k^2$ y como $ij = -ji, ik = -ki, jk = -kj$, se tiene $u^2 = -(\beta^2 + \gamma^2 + \delta^2)e$. Asi $x\,\overline{x} = (\alpha^2 + \beta^2 + \gamma^2 + \delta^2)e = \langle x, x\rangle\, e$.

   $\forall\, x \in \mathbb{H} : x\,\overline{x} = \overline{x}\,x = \langle x, x\rangle\, e$.

5. Dados $x, y \in \mathbb{H}$, de (4) se tiene $(x + y)(x + y) = \langle x + y, x + y\rangle\, e$

   $x\,\overline{x} + x\,\overline{y} + y\,\overline{x} + y\,\overline{y} = (\langle x, x\rangle + \langle x, y\rangle + \langle y, x\rangle + \langle y, y\rangle)\, e$

   $\forall\, x, y \in \mathbb{H}\ : \langle x, y\rangle\, e = \dfrac{1}{2}(x\,\overline{y} + y\,\overline{x})$.

6. Dados $u = \beta i + \gamma j + \delta k, v = \rho i + \sigma j + \tau k \in \mathrm{Im}\mathbb{H}$, se tiene

   $$uv = -(\beta\rho + \gamma\sigma + \delta\tau)e + (\gamma\tau - \delta\sigma)i + (\delta\rho - \beta\tau)j + (\beta\sigma - \gamma\rho)k.$$

   Considerando los vectores $u = (\beta, \gamma, \delta), v = (\rho, \sigma, \tau) \in \mathbb{R}^3$ y teniendo en cuenta el producto escalar y vectorial de $\mathbb{R}^3$ podemos escribir

   $$uv = -\langle u, v\rangle\, e + u \times v, \quad u, v, u \times v \in \mathrm{Im}\mathbb{H}.$$

7. Sean $\alpha e + u, y = \beta e + v \in \mathbb{H}$, se tiene

   $xy = \alpha\beta e + \alpha v + \beta u + uv$

$$xy = \alpha\beta e + \alpha v + \beta u - \langle u, v\rangle e + u \times v$$
$$\overline{xy} = (\alpha\beta - \langle u, v\rangle) e - \alpha v - \beta u - u \times v$$
$$\begin{aligned} \overline{y}\,\overline{x} &= \alpha\beta - \beta u - \alpha v + vu \\ &= \alpha\beta e - \beta u - \alpha v - \langle v, u\rangle e + v \times u \\ &= (\alpha\beta - \langle u, v\rangle) e - \beta u - \alpha v - u \times v \end{aligned}$$
$\forall\, x, y \in \mathbb{H}\colon \overline{xy} = \overline{y}\,\overline{x}$.

8. Dados $x, y \in \mathbb{H}$, se tiene
$$\begin{aligned} \langle x, y\rangle = 0 \ &\Leftrightarrow \frac{1}{2}(x\,\overline{y} + y\,\overline{x}) = 0 \Leftrightarrow x\,\overline{y} = -y\,\overline{x} \Leftrightarrow y\overline{x} = -x\,\overline{y} \\ &\Leftrightarrow \overline{x\,\overline{y}} = -x\,\overline{y} \Leftrightarrow x\,\overline{y} \in \mathbb{H} \end{aligned}$$

2.3. Álgebras Alternativas

2.3.1 Definición. Sea $\mathcal{A}$ un álgebra con elemento unidad e.

1. Se dice que tres elementos u, v, w forman una terna Hamiltoniana si, y solo si, $u^2 = v^2 = w^2 = -e$, $w = uv = -vu$, $u = vw = -wv$, $v = wu = -uw$.

2. El conjunto de elementos imaginarios puros se define como $\mathrm{Im}\mathcal{A} = \{x \in \mathcal{A}; x^2 \in \mathbb{R}e, x \notin \mathbb{R}e - \{0\}\}$.

Es claro que

$$\mathbb{R}e \cap \mathrm{Im}\mathcal{A} = \{0\}, u \in \mathrm{Im}\mathcal{A} \Rightarrow \alpha u \in \mathrm{Im}\mathcal{A} \text{ para todo } \alpha \in \mathbb{R}.$$

2.3.2 Teorema. Si $u, v \in \mathrm{Im}\mathcal{A}$ son linealmente independientes, entonces e, u, v son linealmente independientes.

Prueba.

Consideremos una combinación lineal $\alpha e + \beta u + \gamma v = 0$, donde $\alpha, \beta, \gamma \in \mathbb{R}$. Por demostrar que $\alpha = \beta = \gamma = 0$.
Si $\alpha = 0$, se tiene $\beta = \gamma = 0$ (u y v son linealmente independientes).
Si $\alpha \neq 0$, entonces $\beta \neq 0$ y $\gamma \neq 0$ (caso contrario $u \in \mathbb{R}e$ o $v \in \mathbb{R}e$). En consecuencia, existen $a, b \in \mathbb{R} - \{0\}$ tales que $v = ae + bu$. Por otro lado, $v^2 = a^2e + 2abu + b^2u^2$. Como $u, v \in \mathrm{Im}\mathcal{A}$, se tiene que $2abu = v^2 - a^2e - b^2u^2 \in \mathbb{R}e$, una contradicción (puesto que $ab \neq 0$).$\blacksquare$

2.3.3 Teorema. Si $\mathcal{A}$ no tiene divisores de cero, entonces $u^2 = -we$ con $w > 0$ para todo $u \in \text{Im}\mathcal{A}, u \neq 0$.

Prueba. $u \in \text{Im}\mathcal{A} \Rightarrow u^2 = \alpha e$ para algún $\alpha \in \mathbb{R}$. Supongamos que $\alpha \geq 0$. Luego, existe $\beta \in \mathbb{R}$ tal que $\alpha = \beta^2$. Ahora $(u-\beta e)(u+\beta e) = u^2-\beta^2 e = u^2-\alpha e = 0$. Como $\mathcal{A}$ no tiene divisores de cero, $u = \beta e$ o $u = -\beta e$ contradiciendo que $u \in \text{Im}\mathcal{A}$ con $u \neq 0$.■

2.3.4 Teorema. Si u, v, w es una terna Hamiltoniana en $\mathcal{A}$, entonces

1) la aplicación $f : \mathbb{H} \to \mathcal{A}$ definida por $f((\alpha, \beta, \gamma, \delta)) = \alpha e + \beta u + \gamma v + \delta w$ es un monomorfismo de álgebras.

2) $\mathbb{R}u + \mathbb{R}v + \mathbb{R}w \subset \text{Im}\mathcal{A}$, y en particular $\text{Im}\mathcal{A}$ contiene un subepacio vectorial de dimensión 3.

Prueba.

1) Es claro que f es una aplicación $\mathbb{R}$-lineal. Note que $f(e) = e, f(i) = u, f(j) = v$ y $f(k) = w$. Dados $x, y \in \mathbb{H}$, existen $\alpha, \alpha_1, \beta, \beta_1, \gamma, \gamma_1, \delta, \delta_1 \in \mathbb{R}$ tales que
$x = \alpha e + \beta i + \gamma j + \delta k$ e $y = \alpha_1 e + \beta_1 i + \gamma_1 j + \delta_1 k$.

$$\cdot \quad \begin{aligned} xy &= (\alpha\alpha_1 - \beta\beta_1 - \gamma\gamma_1 - \delta\delta_1)\, e + (\alpha\beta_1 + \beta\alpha_1 + \gamma\delta_1 - \delta\gamma_1)\, i + \\ &\quad (\alpha\gamma_1 - \beta\delta_1 + \gamma\alpha_1 + \delta\beta_1)\, j + (\alpha\delta_1 + \beta\gamma_1 - \gamma\beta_1 + \delta\alpha_1)\, k \end{aligned}$$

$$\cdot \quad \begin{aligned} f(xy) &= (\alpha\alpha_1 - \beta\beta_1 - \gamma\gamma_1 - \delta\delta_1)\, e + (\alpha\beta_1 + \beta\alpha_1 + \gamma\delta_1 - \delta\gamma_1)\, u + \\ &\quad (\alpha\gamma_1 - \beta\delta_1 + \gamma\alpha_1 + \delta\beta_1)\, v + (\alpha\delta_1 + \beta\gamma_1 - \gamma\beta_1 + \delta\alpha_1)\, w \end{aligned}$$

$$\cdot \quad f(x) = \alpha e + \beta u + \gamma v + \delta w \quad ; \quad f(y) = \alpha_1 e + \beta_1 u + \gamma_1 v + \delta_1 w$$

$$\cdot \quad \begin{aligned} f(x)f(y) &= \alpha\alpha_1 e + \alpha\beta_1 u + \alpha\gamma_1 v + \alpha\delta_1 w + \beta\alpha_1 u + \beta\beta_1(-e) + \beta\gamma_1 w \\ &\quad +\beta\delta_1(-v) + \gamma\alpha_1 v + \gamma\beta_1(-w) + \gamma\gamma_1(-e) + \gamma\delta_1 u + \delta\alpha_1 w \\ &\quad +\delta\beta_1 v + \delta\gamma_1(-u) + \delta\delta_1(-e) \\ &= (\alpha\alpha_1 - \beta\beta_1 - \gamma\gamma_1 - \delta\delta_1)\, e + (\alpha\beta_1 + \beta\alpha_1 + \gamma\delta_1 - \delta\gamma_1)\, u + \\ &\quad (\alpha\gamma_1 - \beta\delta_1 + \gamma\alpha_1 + \delta\beta_1)\, v + (\alpha\delta_1 + \beta\gamma_1 - \gamma\beta_1 + \delta\alpha_1)\, w \end{aligned}$$

En consecuencia, se tiene que $f(xy) = f(x)f(y)$ para todo $x, y \in \mathbb{H}$. Es decir, f es un homomorfismo de $\mathbb{R}$-álgebras. Para probar que f es inyectiva, probaremos que e, u, v, w son linealmente independientes.

`Afirmación`.- u y v son linealmente independientes.
Supongamos que u y v son linealmente dependientes. Es decir existe $\alpha \in \mathbb{R}$ tal que $v = \alpha u$. En consecuencia, $uv = u(\alpha u) = (\alpha u)u = vu$.

Como u, v, w es una terna Hamiltoniana se tiene $w = uv = -vu = -uv = -w$, es decir $w = 0$, contradiciendo que $w^2 = -e$. Esto prueba que u y v son linealmente independientes. El teorema (2.3.2) garantiza que e, u, v son linealmente independientes.

Ahora probaremos que e, u, v, w son linealmente independientes. Sea

$$\alpha e + \beta u + \gamma v + \delta w = 0 \quad \text{con} \quad \alpha, \beta, \gamma, \delta \in \mathbb{R}.$$

Si $\delta = 0$, entonces $\alpha = \beta = \gamma = 0$ (e, u, v son linealmente independientes).
Si $\delta \neq 0$, existen $r, s, t \in \mathbb{R}$ tales que $w = re + su + tv$. Como u, v, w es una terna Hamiltoniana, se tiene

$$uv = re + su + tv$$
$$u^2 v = ru + su^2 + tuv$$
$$-v = ru - se + tw.$$

Como e, u, v son linealmente independientes, $t \neq 0$. Por ende $w = \frac{s}{t}e - \frac{r}{t}u - \frac{1}{t}v$.
Como $w = re + su + tv$ y e, u, v son linealmente independientes, se tiene $-\frac{1}{t} = t$ contradiciendo que $t \in \mathbb{R}$. Por tanto, e, u, v, w son linealmente independientes.
2) Sea $ru + sv + tw \in \mathbb{R}u + \mathbb{R}v + \mathbb{R}w$. Como u, v, w es una terna Hamiltoniana, se tiene $(ru + sv + tw)^2 = (-r^2 - s^2 - t^2)\, e \in \mathbb{R}e$.■

2.3.5 Teorema. Sea $\mathcal{A}$ un álgebra sin divisores de cero. Si U es un subespacio vectorial de $\mathrm{Im}\mathcal{A}$ de dimensión dos, entonces para todo $p \in U$ existe un $q \in U \setminus \mathbb{R}p$ tal que $pq + qp = 0$.

Prueba. Sea $p \in U \setminus \{0\}$. Como $U \subset \mathrm{Im}\mathcal{A}$, existe $\alpha \neq 0$ tal que $p^2 = \alpha e$.
`Afirmación`.- Dado $x \in U$ tal que p y x son linealmente independientes, existe $\beta \in \mathbb{R}$ tal que $px + xp = \beta e$.
En efecto, $(p + x)^2 = p^2 + px + xp + x^2$. Como $p, x, p + x \in U \subset \mathrm{Im}\mathcal{A}$, existe $\beta \in \mathbb{R}$ tal que $px + xp = \beta e$.

De la afirmación, cuando $\beta = 0$, basta elegir $q = x$.

Si $\beta \neq 0$, dado $q \in U$ existen $r, s \in \mathbb{R}$ tales que $q = rx + sp$. Note que $q \notin \mathbb{R}p$ si, y solo si, $r \neq 0$. Es decir, existe $z \in U$ linealmente independiente con p tal que $q = z + sp$. Ahora se tiene,

$$\begin{aligned} pq + qp = 0 &\Leftrightarrow p(z + sp) + (z + sp)p = 0 \\ &\Leftrightarrow pz + sp^2 + zp + sp^2 = 0 \\ &\Leftrightarrow pz + zp + 2sp^2 = 0. \end{aligned}$$

Por la afirmación, existe $\beta \in \mathbb{R}$ tal que $pz + zp = \beta e$. En consecuencia,

$$\beta e + 2sp^2 = 0 \Leftrightarrow \beta + 2\alpha s = 0.$$

Bastará elegir $q = z + sp$, donde $s = -\dfrac{\beta}{2\alpha}$.■

2.3.6 Definición. Se dice que un álgebra $\mathcal{A}$ es alternativa si, y solo si, $x(xy) = x^2y$ y $(xy)y = xy^2$ para todo $x, y \in \mathcal{A}$.

2.3.7 Nota. Es claro que

1. Toda álgebra asociativa es alternativa.
2. Si $\mathcal{A}$ es alternativa, entonces $(xy)x = x(yx)$ para todo $x, y \in \mathcal{A}$.
3. Dos cualesquiera de las identidades $x(xy) = x^2y, (xy)y = xy^2, (xy)x = x(yx)$ juntas, implican la tercera.

2.3.8 Teorema (Existencia de ternas Hamiltonianas)**.** Sea $\mathcal{A}$ un álgebra alternativa sin divisores de cero, con elemento unidad. Si U es un subespacio vectorial de $\mathrm{Im}\mathcal{A}$ de dimensión dos, entonces para todo elemento $u \in \mathcal{A}$ tal que $u^2 = -e$ existe $v \in U$ tal que u, v, uv forman una terna Hamiltoniana.

Prueba. Sea $u \in U$ tal que $u^2 = -e$. Por (2.3.5) existe $p \in U \setminus \mathbb{R}u$ con $p \neq 0$ tal que $up + pu = 0$. Como $\mathcal{A}$ no tiene divisores de cero, existe $r > 0$ tal que $p^2 = -re$ (ver 2.3.3). Es decir, existe $v = \dfrac{1}{\sqrt{r}}p \in U$ tal que $v^2 = -e$ y $uv = -vu$. Sea $w := uv$. Como $\mathcal{A}$ es un álgebra alternativa, se tiene $vw = v(uv) = -v(vu) = -v^2u = u$, $wv = (uv)v = uv^2 = -u$, $wu = (uv)u = (-vu)u = v$, $uw = u(uv) = u^2v = -v$.

Resta probar que $w^2 = -e$. Note que $vw^2 = (vw)w = uw = -v$. Luego, $vw^2 + v = 0 \Leftrightarrow v(w^2 + e) = 0$. Como $\mathcal{A}$ no tiene divisores de cero, se concluye que $w^2 = -e$.■

2.3.9 Nota. Toda álgebra alternativa $\mathcal{A}$, es una potencia asociativa.

2.3.10 Teorema. Toda álgebra alternativa de división $\mathcal{A}$ de dimensión finita tiene elemento unidad.

Prueba. Sea $a \in \mathcal{A}$ con $a \neq 0$. Como $\mathcal{A}$ es un álgebra de división existe un (único)$e \in \mathcal{A}$ tal que $ea = a$. Ahora $a \neq 0$, garantiza que $e \neq 0$. Como $\mathcal{A}$ es alternativa $ea = e(ea) = e^2a$. Es decir, $(e - e^2)a = 0$ y como $\mathcal{A}$ no tiene divisores de cero, $e^2 = e$.
Sea $x \in \mathcal{A}$. Como $e^2 = e$ se tiene

$$\begin{aligned} e^2 - e = 0 &\Leftrightarrow (e^2 - e)x = 0x \\ &\Leftrightarrow e^2x - ex = 0 \\ &\Leftrightarrow e(ex) - ex = 0 \quad (\mathcal{A}\,\text{es alternativa}) \\ &\Leftrightarrow e(ex - x) = 0 \end{aligned}$$

Como $e \neq 0$, se tiene $ex = x$. Analogamente,

$$\begin{aligned} x(e^2 - e) = 0 &\Leftrightarrow xe^2 - xe = 0 \\ &\Leftrightarrow (xe)e - xe = 0 \\ &\Leftrightarrow (xe - x)e = 0 \\ &\Leftrightarrow xe = x \end{aligned}$$

Por lo tanto, $xe = x$ y $ex = x$ para todo $x \in \mathcal{A}$.■

2.3.11 Definición. Se dice que un álgebra $\mathcal{A}$ con elemento unidad e es un álgebra cuadrática si, y solo si, para todo $x \in \mathcal{A}$ existen $\alpha, \beta \in \mathbb{R}$ tales que $x^2 = \alpha e + \beta x$.

Las álgebras $\mathbb{C}$ y $\mathbb{H}$ son cuadráticas (ver 2.2.4).

2.3.12 Teorema. Si $\mathcal{A}$ es un álgebra cuadrática, entonces $\mathrm{Im}\mathcal{A}$ es un subespacio vectorial de $\mathcal{A}$ y $\mathcal{A} = \mathbb{R}e \oplus \mathrm{Im}\mathcal{A}$.

Prueba.

1) Bastará probar que $u, v \in \mathrm{Im}\mathcal{A} \Rightarrow u + v \in \mathrm{Im}\mathcal{A}$.

`Caso` 1. $u, v \in \mathrm{Im}\mathcal{A}$ linealmente dependientes.

Como u y v son linealmente independientes, existe $\alpha \in \mathbb{R}$ tal que $v = \alpha u$. Luego, $u + v = (1 + \alpha)u \in \mathrm{Im}\mathcal{A}$.

`Caso` 2. $u, v \in \mathrm{Im}\mathcal{A}$ linealmente independientes.

Como $\mathcal{A}$ es un álgebra cuadrática, existen $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{R}$ tales que

$$(u + v)^2 = \alpha_1 e + \beta_1(u + v) \quad \text{y} \quad (u - v)^2 = \alpha_2 e + \beta_2(u - v).$$

Desarrollando ambas expresiones obtenemos,

$u^2 + uv + vu + v^2 = \alpha_1 e + \beta_1 u + \beta_1 v$

$u^2 - uv - vu + v^2 = \alpha_2 e + \beta_2 u - \beta_2 v$

Sumando estas expresiones se tiene

$$(\beta_1 + \beta_2)u + (\beta_1 - \beta_2)v = 2u^2 + 2v^2 - (\alpha_1 + \alpha_2)e.$$

Como $u, v \in \mathrm{Im}\mathcal{A}$, existe $\lambda \in \mathbb{R}$ tal que $(\beta_1 + \beta_2)u + (\beta_1 - \beta_2)v = \lambda e$.

Ahora (2.3.2) garantiza que $\beta_1 + \beta_2 = 0 = \beta_1 - \beta_2$. Es decir, $(u + v)^2 = \alpha_1 e$. Como e, u, v son linealmente independientes, se concluye que $u + v \notin \mathbb{R}e$. Por lo tanto, $u + v \in \mathrm{Im}\mathcal{A}$.

2) Sea $x \in \mathcal{A}$ tal que $x \notin \mathbb{R}e$. Como $\mathcal{A}$ es un álgebra cuadrática, existen $\alpha, \beta \in \mathbb{R}$ tales que $x^2 = \alpha e + 2\beta x$. Entonces, $(x - \beta e)^2 = x^2 - 2\beta x + \beta^2 e = (\alpha + \beta^2)e$ y como $x - \beta e \notin \mathbb{R}e$, existe $u \in \mathrm{Im}\mathcal{A}$ tal que $u = x - \beta e$. Asi $\mathcal{A} = \mathbb{R}e + \mathrm{Im}\mathcal{A}$ y como $\mathbb{R}e \cap \mathrm{Im}\mathcal{A} = \{0\}$, se tiene $\mathcal{A} = \mathbb{R}e \oplus \mathrm{Im}\mathcal{A}$.$\blacksquare$

Sea $\mathcal{A}$ una potencia asociativa con elemento unidad e, para cualquier polinomio $f = \alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n \in \mathbb{R}[X]$ definimos $f(x)$ por

$f(x) := \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n \in \mathcal{A}$ (es decir, sustituyendo $x \in \mathcal{A}$ por X). Entonces $(f.g)(x) = f(x)g(x)$ para todo polinomio $f, g \in \mathbb{R}[X]$ y para todo $x \in \mathcal{A}$.

`Ley de Sustitución`:

Si $\mathcal{A}$ es una potencia asociativa y tiene un elemento unidad, entonces todo elemento $x \in \mathcal{A}$ define un homomorfismo de álgebras mediante la aplicación $\mathbb{R}[X] \to \mathcal{A}$, $f \mapsto f(x)$ (llamado homomorfismo de sustitución correspondiente a x).

2.3.13 Teorema. Toda álgebra alternativa finito dimensional $\mathcal{A}$ es cuadrática.

Prueba. Se tiene que $\mathcal{A}$ es una potencia asociativa con elemento unidad e (ver 2.3.9). Luego para cada $x \in \mathcal{A}$ el homomorfismo de sustitución $\mathbb{R}[X] \to \mathcal{A}$, $f \mapsto f(x)$ queda bien establecido; es claro que su núcleo es un ideal principal, pues $\mathbb{R}[X]$ es un anillo de ideales principales. Como $\dim\mathcal{A} < +\infty$, este ideal principal no es el ideal cero y como $\mathcal{A}$ no tiene divisores de cero, este núcleo es un ideal primo. En consecuencia existe un polinomio primo mónico $p \in \mathbb{R}[X]$ tal que $p(x) = 0$. Como todo polinomio mónico primo en $\mathbb{R}[X]$ es de la forma $X - \gamma$ o $X^2 - \beta X - \alpha$, se concluye que $x = \gamma$ o $x^2 - \beta x - \alpha = 0$ para todo $\alpha, \beta, \gamma \in \mathcal{A}$.■

2.3.14 Teorema. Sea $\mathcal{A}$ un álgebra alternativa, cuadrática sin divisores de cero. Si $\dim\mathcal{A} \geq 3$, entonces $\mathcal{A}$ contiene una terna Hamiltoniana y subálgebras $\mathcal{B}$ con $e \in \mathcal{B}$ isomorfas al álgebra de cuaterniones $\mathbb{H}$.

Prueba. Por (2.3.12), $\mathrm{Im}\mathcal{A}$ es un subespacio vectorial de $\mathcal{A}$ y $\mathcal{A} = \mathbb{R}e \oplus \mathrm{Im}\mathcal{A}$. Es claro que $\dim(\mathrm{Im}\mathcal{A}) \geq 2$. Ahora (2.3.8) garantiza que existe una terna Hamiltoniana $u, v, w \in \mathcal{A}$ y en consecuencia existe una subálgebra $\mathcal{B}$ con $e \in \mathcal{B}$ isomorfa a $\mathbb{H}$.■

2.3.15 Teorema (de Frobenius)**.** Sea $\mathcal{A} \neq 0$ un álgebra real asociativa, cuadrática sin divisores de cero.

1. Si $\dim(\mathcal{A}) = 1$, entonces $\mathcal{A}$ es isomorfa al álgebra $\mathbb{R}$ de los números reales.

2. Si $\dim(\mathcal{A}) = 2$, $\mathcal{A}$ es isomorfa al álgebra $\mathbb{C}$ de los números complejos.

3. Si $\dim(\mathcal{A}) \geq 3$, $\mathcal{A}$ es isomorfa al álgebra $\mathbb{H}$ de los cuaterniones.

Prueba. Sea e el elemento unidad de $\mathcal{A}$ en cada caso.

1. Como $\dim\mathcal{A} = 1$, entonces $\mathcal{A}$ es isomorfa a $\mathbb{R}$ (ver 1.1.7).

2. Como $\dim\mathcal{A} = 2$, existe $u \in \mathcal{A}$ tal que $u^2 = -e$. Sea $f : \mathbb{C} \to \mathcal{A}$ definida por $f(x+iy) = xe + yu$. Es claro que f es un homomorfismo de $\mathbb{R}$-álgebras. Como e y u son linealmente independientes, f es inyectiva y como $\dim\mathbb{C} = \dim\mathcal{A}$, es claro que f es biyectiva. Por tanto, f es un isomorfismo de álgebras.

3. Como $\dim\mathcal{A} \geq 3$, por (2.3.14) existe una terna Hamiltoniana $u, v, w \in \mathrm{Im}\mathcal{A}$ tal que
$w = uv$. Sea $x \in \mathrm{Im}\mathcal{A}$ arbitrario. Como $u, x, x+u \in \mathrm{Im}\mathcal{A}$ y
$xu+ux = (x+u)^2 - x^2 - u^2$, $xu+ux \in \mathbb{R}e$. Intercambiando u por v y w, se tiene que existen $\alpha, \beta, \gamma \in \mathbb{R}$ tales que $xu+ux = \alpha e$, $xv+vx = \beta e$, $xw+wx = \gamma e$. Ahora,
$$\begin{cases} (xu+ux)v = (\alpha e)v & \Rightarrow xw + u(xv) = \alpha v \\ u(xv+vx) = u(\beta e) & \Rightarrow u(xv) + wx = \beta u \end{cases}$$
Restando obtenemos, $xw - wx = \alpha v - \beta u$ y sumando está última igualdad con $xw + wx = \gamma e$, se tiene $2xw = \alpha v - \beta u + \gamma e$. De $(2xw)w = (\alpha v - \beta u + \gamma e)w$, se concluye que $x = -\frac{\alpha}{2}u - \frac{\beta}{2}v - \frac{\gamma}{2}w \in \mathbb{R}u + \mathbb{R}v + \mathbb{R}w$. Es decir,
$\mathrm{Im}\mathcal{A} = \mathbb{R}u + \mathbb{R}v + \mathbb{R}w$ (ver 2.3.4). Por ende, $\dim(\mathrm{Im}\mathcal{A}) = 3$. Por (2.3.12), $\mathcal{A} = \mathbb{R}e \oplus \mathrm{Im}\mathcal{A}$. Como $\dim\mathcal{A} = 4$, (2.3.14) garantiza que $\mathcal{A}$ es isomorfa a $\mathbb{H}$.■

2.3.16 Corolario. Toda álgebra real $\mathcal{A}$ de división de dimensión finita, asociativa y sin divisores de cero, es isomorfa a $\mathbb{H}$.■

Capítulo 3

Los Números de Cayley $\mathbb{O}$

3.1. Álgebras alternativas cuadráticas

En 2.3.12 se probó que toda álgebra real cuadrática $\mathcal{A}$ tiene la propiedad $\mathcal{A} = \mathbb{R}e \oplus \mathrm{Im}\mathcal{A}$ y que $\mathrm{Im}\mathcal{A}$ es un subespacio vectorial de $\mathcal{A}$. Este hecho nos permite definir la aplicación $\mathbb{R}$-lineal $\lambda : \mathcal{A} \to \mathbb{R}$ por $\lambda(e) = 1$ y $\mathrm{Nuc}(\lambda) = \mathrm{Im}\mathcal{A}$ llamada forma lineal del álgebra cuadrática.
Ahora, dada un $\mathbb{R}$-álgebra cuadrática $\mathcal{A}$ definimos la aplicación

$$^{-} : \mathcal{A} \to \mathcal{A}, \ x \mapsto \overline{x} = 2\lambda(x)e - x.$$

Es claro que esta aplicación es $\mathbb{R}$-lineal y $\overline{x} = \lambda(x)e - u$ para $x = \lambda(x)e + u$ con $u \in \mathrm{Im}\mathcal{A}$. Note que $x \mapsto \overline{x}$ es una reflexión de $\mathcal{A}$ con respecto a la línea $\mathbb{R}e$.
El conjunto de los puntos fijos $\{x \in \mathcal{A}; \overline{x} = x\}$ es la $\mathbb{R}$-subálgebra $\mathbb{R}e$. En efecto,

$$\overline{x} = x \Leftrightarrow 2\lambda(x)e - x = x \Leftrightarrow x = \lambda(x)e \in \mathbb{R}e.$$

3.1.1 Teorema. Sea $\mathcal{A}$ un álgebra cuadrática cuya forma lineal es λ. Entonces $\langle\, , \rangle : \mathcal{A} \times \mathcal{A} \to \mathbb{R}$ dada por $\langle x, y\rangle = 2\lambda(x)\lambda(y) - \dfrac{1}{2}\lambda\,(xy + yx)$ es una forma bilineal simétrica y para todo $x, y \in \mathcal{A}$ se cumple

1) $\langle x, x\rangle = 2\lambda(x)^2 - \lambda(x^2)$

2) $\langle x, e\rangle = \lambda(x), \ \langle e, e\rangle = 1$

3) $x^2 = 2\lambda(x)x - \langle x, x\rangle\, e$

4) $xy + yx = 2\lambda(x)y + 2\lambda(y)x - 2\langle x, y\rangle e$

Si $\mathcal{A}$ no tiene divisores de cero, entonces $\langle x, x\rangle > 0$ para todo $x \neq 0$.

Prueba.

Como $\lambda(x) \in \mathbb{R}$ para $x \in \mathcal{A}$, es claro que $\langle\, ,\rangle$ es simétrica.

Como λ es $\mathbb{R}$-lineal, es claro que la aplicación $\langle\, ,\rangle : \mathcal{A}\times\mathcal{A} \to \mathbb{R}$ es una forma bilineal.

Por definición de $\langle\, ,\rangle$, es claro que (1) y (2) se cumplen.

3) Dado $x \in \mathcal{A}$, es claro que

$$0 = \lambda(x) - \lambda(x) = \lambda(x) - \lambda(x)\lambda(e) = \lambda(x) - \lambda(\lambda(x)e) = \lambda(x - \lambda(x)e).$$

Es decir, $x - \lambda(x)e \in \mathrm{Nuc}(\lambda) = \mathrm{Im}\mathcal{A}$. Por definición de $\mathrm{Im}\mathcal{A}$, existe $w(x) \in \mathbb{R}$ tal que

$$(x - \lambda(x)e)^2 = -w(x)e \tag{3.1}$$

De (3.1) obtenemos, $x^2 = 2\lambda(x)x - [\lambda(x)^2 + w(x)]\, e$. Como $\lambda(x), w(x) \in \mathbb{R}$, aplicando λ se tiene $\lambda(x^2) = \lambda(x)^2 - w(x)$. De esta última ecuación y del resultado (1), se tiene $\langle x, x\rangle = \lambda(x)^2 + w(x)$. Sustituyendo $w(x) = \langle x, x\rangle - \lambda(x)^2$ en (3.1) se concluye que

$$x^2 = 2\lambda(x)x - \langle x, x\rangle e.$$

4) Si $\mathcal{A}$ no tiene divisores de cero, por (2.3.3) para $x \in \mathcal{A}$ con $x \neq 0$ existe $w(x) \geq 0$ tal que

$$(x - \lambda(x))^2 = -w(x)e \tag{3.2}$$

Si $\langle x, x\rangle = 0$, $\lambda(x)^2 + w(x) = 0$. Como $\lambda(x), w(x) \in \mathbb{R}$, $\lambda(x) = 0 = w(x)$. Ahora la ecuación (3.2), garantiza que $x = 0$; contradiciendo que $x \neq 0$. En consecuencia, $\langle x, x\rangle > 0$ para todo $x \neq 0$.

Como $x^2 = 2\lambda(x)x - \langle x, x\rangle e$ para todo $x \in \mathcal{A}$, para $x + y \in \mathcal{A}$ se tiene $(x + y)^2 = 2\lambda(x + y)(x + y) - \langle x + y, x + y\rangle e$. De está expresión, considerando (3), la linealidad de λ y la binealidad de $\langle\, ,\rangle$, se concluye que

$$xy + yx = 2\lambda(x)y + 2\lambda(y)x - 2\langle x, y\rangle e. \blacksquare$$

La forma bilineal $\langle\, ,\rangle : \mathcal{A} \times \mathcal{A} \to \mathbb{R}$ es llamada forma bilineal del álgebra cuadrática $\mathcal{A}$.

3.1.2 Corolario. Para todo $x, y \in \mathrm{Im}\mathcal{A}$, se tiene $xy + yx = -2\langle x, y\rangle e$. En particular, $\langle x, y\rangle = 0$ si, y solo si, $xy + yx = 0$.

Prueba. Es consecuencia directa de (4) de (3.1.1).$\blacksquare$

3.1.3 Corolario. Para todo $x, y, z \in \mathrm{Im}\mathcal{A}$, se tiene

1) $xy \cdot z + yx \cdot z = -2\langle x, y\rangle z$

2) $y \cdot xz + y \cdot zx = -2\langle x, z\rangle y$

3) $x \cdot yz + yz \cdot x = 2\lambda(yz)x - 2\langle x, yz\rangle e$

Prueba.
1) Por (3.1.2) se tiene, $xy + yx = -2\langle x, y\rangle e$. Luego, $xy \cdot z + yx \cdot z = -2\langle x, y\rangle z$.
2) Por (3.1.2) se tiene, $xz + zx = -2\langle x, z\rangle e$. Por tanto, $y \cdot xz + y \cdot zx = -2\langle x, z\rangle y$.
3) Sustituyendo y por yz en (4) de (3.1.1), se tiene

$$x \cdot yz + yz \cdot x = 2\lambda(x)y + 2\lambda(yz)x - 2\langle x, yz\rangle e.\blacksquare$$

3.1.4 Teorema. Si $\mathcal{A}$ es un álgebra alternativa cuadrática, entonces para todo $x, y, z \in \mathcal{A}$ se cumple

1) $\lambda(xy) = \lambda(yx)$, $\langle x, y\rangle = 2\lambda(x)\lambda(y) - \lambda(xy)$

2) $\lambda(xyz) := \lambda(xy \cdot z) = \lambda(x \cdot yz)$ (asociativiada de λ)

3) $\langle xy, z\rangle + \langle xz, y\rangle = 2\lambda(x)\langle y, z\rangle$

4) $\langle xy, xy\rangle = \langle x, x\rangle \langle y, y\rangle$ (regla del producto)

Si la forma bilineal de $\mathcal{A}$ es definida positiva, entonces $\mathcal{A}$ no tiene divisores de cero.

Prueba. Como las identidades multilineales (1), (2) o (3) no cambian si se añaden multiplos escalares de e a elementos arbitrarios de $\mathcal{A}$, podemos asumir sin restricción en la prueba que $x, y, z \in \mathrm{Im}\mathcal{A}$ y se tiene $\lambda(x) = \lambda(y) = \lambda(z) = 0$. Haciendo $z = x$ en (1) y (3) de (3.1.3), se obtiene

$$xy \cdot x + yx \cdot x = -2\langle x, y\rangle x \quad \text{y} \quad x \cdot yx + yx \cdot x = 2\lambda(yx)x - 2\langle x, yx\rangle e.$$

$$0 = xy \cdot x - x \cdot yx = -2\langle x, y\rangle x - 2\lambda(yx)x + 2\langle x, yx\rangle e$$

$$0 = -2(\langle x, y\rangle + \lambda(yx))x + 2\langle x, yx\rangle e$$

En consecuencia, $\langle x, y\rangle + \lambda(yx) = 0$ y $\langle x, yx\rangle = 0$ para todo $x, y \in \mathrm{Im}\mathcal{A}$.

1) Sustituyendo x por $x+y$ en $\langle x, y\rangle+\lambda(yx) = 0$, se tiene $\langle x, y\rangle+\langle y, y\rangle+\lambda(yx+y^2) = 0$ y de (3.1.1) se concluye que

$$2\lambda(x)\lambda(y) - \frac{1}{2}\lambda(xy) - \frac{1}{2}\lambda(yx) + 2\lambda(y)^2 - \lambda(y^2) + \lambda(yx) + \lambda(y^2) = 0.$$

En consecuencia, $\lambda(xy) = \lambda(yx)$. De esta igualdad y de (3.1.1), se tiene

$$\langle x, y\rangle = 2\lambda(x)\lambda(y) - \frac{1}{2}[\lambda(xy) + \lambda(yx)].$$

Por lo tanto, $\langle x, y\rangle = 2\lambda(x)\lambda(y) - \lambda(xy)$.

2) Como $\mathcal{A}$ es alternativa, se tiene que $\lambda(x \cdot yx) = \lambda(xy \cdot x)$ para todo $x, y \in \mathcal{A}$. Sustituyendo x por $x + z$, obtenemos

$$\lambda((x + z) \cdot y(x + z)) = \lambda((x + z)y \cdot (x + z))$$

$$\lambda((x + z)(yx + yz)) = \lambda((xy + zy)(x + z))$$

Usando la linealidad de λ, se obtiene

$$\lambda(x \cdot yz) + \lambda(z \cdot yx) = \lambda(xy \cdot z) + \lambda(zy \cdot x) \qquad (*)$$

para todo $x, y, z \in \mathrm{Im}\mathcal{A}$.

Ahora de (1) y (2) de (3.1.3), se tiene

$$zy \cdot x + yz \cdot x = -2\langle z, y\rangle x \quad \text{y} \quad z \cdot yx + z \cdot xy = -2\langle y, x\rangle z$$

respectivamente. Luego, $\lambda(zy\cdot x) = -\lambda(yz\cdot x)$ y $\lambda(z\cdot yx) = -\lambda(z\cdot xy)$. Reemplazando estas expresiones en $(*)$ obtenemos $\lambda(x \cdot yz) - \lambda(z \cdot xy) = \lambda(xy \cdot z) - \lambda(yz \cdot x)$. Como $\lambda(x \cdot yz) = \lambda(yz \cdot x)$ y $\lambda(xy \cdot z) = \lambda(z \cdot xy)$, se concluye que $\lambda(xy \cdot z) = \lambda(x \cdot yz)$.

3) Sustituyendo x por xy en $\langle x, y\rangle + \lambda(xy) = 0$, se tiene $\langle xy, y\rangle + \lambda(xy \cdot y) = 0$. Ahora reemplazando y por $y + z$, obtenemos

$$\langle x(y + z), y + z\rangle + \lambda(x(y + z) \cdot (y + z)) = 0$$

$$\langle xy + xz, y + z\rangle + \lambda\left(x(y + z)^2\right) = 0$$

$$\langle xy, y\rangle + \langle xy, z\rangle + \langle xz, y\rangle + \langle xz, z\rangle + \lambda\left(x(y^2 + yz + zy + z^2)\right) = 0$$

$$\langle xy, z\rangle + \langle xz, y\rangle + \lambda\left(xy^2 + x(yz + zy) + xz^2\right) = 0$$

Utilizando (4) de (3.1.1) en esta última ecuación, obtenemos

$\langle xy, z\rangle + \langle xz, y\rangle = 2\langle y, z\rangle \lambda(x)$.

4) Haciendo $z = xy$ en (3), se tiene $\langle xy, xy\rangle + \langle x \cdot xy, y\rangle = 2\lambda(x)\langle y, xy\rangle$. Como $\mathcal{A}$ es alternativa, $\langle xy, xy\rangle + \langle x^2y, y\rangle = 2\lambda(x)\langle y, xy\rangle$. Por otro lado,

$$\begin{aligned}
\langle xy, xy\rangle &= 2\lambda(x)\langle y, xy\rangle - \left\langle x^2y, y\right\rangle \\
&= \left\langle 2\lambda(x)xy - x^2y, y\right\rangle \\
&= \langle 2\lambda(x)xy - (2\lambda(x)x - \langle x, x\rangle e)y, y\rangle \text{ (ver 3.1.1)}
\end{aligned}$$

por lo tanto, $\langle xy, xy\rangle = \langle x, x\rangle \langle y, y\rangle$.■

3.1.5 Nota. Sea $\mathcal{A}$ una álgebra alternativa cuadrática.

1. Si la forma bilineal de $\mathcal{A}$ es definida positiva, entonces $\mathcal{A}$ no tiene divisores de cero. En efecto, supongamos que existen $x, y \in \mathcal{A} - \{0\}$ tales que $xy = 0$. Por (4) de (3.1.4), $\langle x, x\rangle = 0$ o $\langle y, y\rangle = 0$. Contradiciendo que, $\langle\,,\rangle$ es definida positiva.

2. En $\lambda(xy \cdot z) = \lambda(x \cdot yz)$ reemplazando x por y e y por x, obtenemos
   $\lambda(yx \cdot z) = \lambda(y \cdot xz)$. Ahora por (1), $\lambda(yx \cdot z) = \lambda(xz \cdot y)$.
   Ahora cambiando x por z y z por x, se tiene $\lambda(yz \cdot x) = \lambda(zx \cdot y)$.
   Procediendo analogamente, de (1) y (2) se tiene que

$$\lambda(xyz) := \lambda(xy \cdot z) = \lambda(yz \cdot x) = \lambda(zx \cdot y)$$

   para todo $x, y, z \in \mathcal{A}$.

3.1.6 Corolario. Dada $\mathcal{A}$ álgebra alternativa cuadrática, las siguientes afirmaciones son equivalentes para $x, y \in \mathrm{Im}\mathcal{A}$

1. $\langle x, y\rangle = 0$
2. $xy + yx = 0$
3. $\lambda(xy) = 0$

Prueba.

(1) $\Leftrightarrow$ (2), es inmediato por (3.1.2).

(1) $\Leftrightarrow$ (3), consecuencia directa de (1) de (3.1.4).■

3.1.7 Teorema. Sea $\mathcal{A}$ un álgebra cuadrática. Para todo $x, y, z \in \mathcal{A}$, se verifica

1. $\overline{xy} = \overline{y}\,\overline{x}$

2. $x\,(\overline{x}y) = \overline{x}(xy) = \langle x, x\rangle\, y$, en particular $x\overline{x} = \overline{x}x = \langle x, x\rangle\, e$.

3. $\langle x, y\rangle = \lambda\,(x\overline{y}) = \lambda\,(\overline{x}y)$, en particular $\langle xy, z\rangle = \langle x, z\,\overline{y}\rangle = \langle y, \overline{x}z\rangle$.

Prueba.

$$
\begin{aligned}
1.\ \overline{xy} - \overline{y}\,\overline{x} &= 2\lambda(xy)e - xy - (2\lambda(y)e - y)\,(2\lambda(x)e - x)\\
&= 2\lambda(xy)e - xy - [4\lambda(x)\lambda(y)e - 2\lambda(y)x - 2\lambda(x)y + yx]\\
&= 2\,(\lambda(xy) - 2\lambda(x)\lambda(y))\,e + 2\lambda(x)y + 2\lambda(y)x - (xy + yx).
\end{aligned}
$$

Como $\lambda(xy) - 2\lambda(x)\lambda(y) = -\langle x, y\rangle$ (ver 1 de 3.1.4) y

$2\lambda(x)y+2\lambda(y)x-(xy+yx) = 2\,\langle x, y\rangle\, e$ (ver 4 de 3.1.1), se concluye que $\overline{xy}-\overline{y}\,\overline{x} = 0$.

$$
\begin{aligned}
2.\ x\,(\overline{x}y) &= x\,([2\lambda(x)e - x]y) = x\,(2\lambda(x)y - xy)\\
&= 2\lambda(x)xy - x\cdot xy = 2\lambda(x)xy - x^2y\\
&= (2\lambda(x) - x^2)\,y = \langle x, x\rangle\, ey = \langle x, x\rangle\, y
\end{aligned}
$$

$$
\begin{aligned}
\overline{x}(xy) &= (2\lambda(x)e - x)\,xy = 2\lambda(x)xy - x\cdot xy\\
&= 2\lambda(x)xy - x^2y = (2\lambda(x)x - x^2)\,y = \langle x, x\rangle\, y
\end{aligned}
$$

3. Como $x = 2\lambda(x)e - \overline{x}$, se tiene $xy = 2\lambda(x)y - \overline{x}y$. Es decir,

$\lambda(xy) = 2\lambda(x)\lambda(y) - \lambda\,(\overline{x}y)$. Ahora por (1) de (3.1.4), se tiene

$2\lambda(x)\lambda(y)-\langle x, y\rangle = 2\lambda(x)\lambda(y)-\lambda(\overline{x}y)$. En consecuencia, $\lambda(\overline{x}y) = \langle x, y\rangle$. Procediendo analogamente, se concluye que $\lambda(x\overline{y}) = \langle x, y\rangle$. Por lo tanto,

$\langle x, y\rangle = \lambda(\overline{x}y) = \lambda(x\overline{y})$.

Finalmente,

$$
\begin{aligned}
\langle xy, z\rangle &= \left\langle xy, \overline{\overline{z}}\,\right\rangle = \lambda\,(xy\cdot\overline{z}) = \lambda\,(x\cdot y\,\overline{z}) \quad \text{(por 2 de 3.1.4)}\\
&= \lambda\left(x\cdot\overline{z\,\overline{y}}\,\right) = \langle x, z\,\overline{y}\rangle\,.
\end{aligned}
$$

$$
\begin{aligned}
\langle y, \overline{x}\,z\rangle &= \left\langle y, \overline{\overline{z}\,x}\,\right\rangle = \lambda(y\cdot\overline{z}x) = \lambda(y\overline{z}\cdot x)\\
&= \langle z\,\overline{y}, x\rangle = \langle x, z\,\overline{y}\rangle\,.
\end{aligned}
$$

En consecuencia, $\langle xy, z\rangle = \langle x, z\,\overline{y}\rangle = \langle y, \overline{x}z\rangle$.■

3.1.8 Teorema. Si $\mathcal{A}$ es un álgebra alternativa cuadrática, entonces

$$xy\cdot z + x\cdot yz = 2\lambda(yz)x - 2\lambda(xz)y + 2\lambda(xy)z + 2\lambda(xyz)e$$

para todo $x, y, z \in \mathrm{Im}\mathcal{A}$.

Prueba. Como $\mathcal{A}$ es alternativa, se tiene $yx \cdot x = yx^2$. Ahora sustituyendo x por $x+z$, obtenemos

$y(x+z)\cdot(x+z) = y\cdot(x+z)(x+z)$

$(yx+yz)(x+z) = y\left[(x+z)x+(x+z)z\right]$

$(yx+yz)x+(yx+yz)z = y(x^2+zx+xz+z^2)$

$yx\cdot x+yz\cdot x+yx\cdot z+yz\cdot z = y\cdot x^2+y\cdot zx+y\cdot xz+yz^2$. Es decir,

$$yx\cdot z+yz\cdot x = y\cdot xz+y\cdot zx \tag{$*$}$$

para $x,y,z\in\mathcal{A}$. Ahora para $x,y,z\in \mathrm{Im}\mathcal{A}$ de (3.1.3), se tiene

$(xy\cdot z+yx\cdot z)-(y\cdot xz+y\cdot zx)+(x\cdot yz+yz\cdot x) = -2\langle x,y\rangle z +$

$2\langle x,z\rangle y+2\lambda(yz)x-2\langle x,yz\rangle e$.

De esta última igualdad y teniendo en cuenta $(*)$, se obtiene

$$xy\cdot z+x\cdot yz = -2\langle x,y\rangle z+2\langle x,z\rangle y+2\lambda(yz)x-2\langle x,yz\rangle e.$$

Finalmente usando (3.1.4) obtenemos

$$\begin{aligned} xy\cdot z+x\cdot yz &= -2\left[2\lambda(x)\lambda(y)-\lambda(xy)\right]z+2\left[2\lambda(x)\lambda(z)-\lambda(xz)\right]y+ \\ &\quad 2\lambda(yz)x-2\left[2\lambda(x)\lambda(yz)-\lambda(x\cdot yz)\right]e \\ &= 2\lambda(yz)x-2\lambda(xz)y+2\lambda(xy)z+2\lambda(x\cdot yz)e.\blacksquare \end{aligned}$$

3.1.9 Corolario. Si $x,y,z\in \mathrm{Im}\mathcal{A}$ son ortogonales dos a dos, entonces $xy\cdot z = -zy\cdot x$.

Prueba. Como $x,y,z\in \mathrm{Im}\mathcal{A}$ son ortogonales dos a dos, de (3.1.6) se tiene $\lambda(xy)=\lambda(xz)=\lambda(yz)=0$. Por otro lado, (3.1.8) garantiza que $xy\cdot z+x\cdot yz = 2\lambda(x\cdot yz)e$. Ahora,

$$xy\cdot z = 2\lambda(x\cdot yz)e - x\cdot yz = \overline{x\cdot yz} = \overline{yz}\cdot\overline{x} = \overline{z}\,\overline{y}\cdot\overline{x} = -zy\cdot x\,.\blacksquare$$

Dada un álgebra $\mathcal{B}$ la expresión $\langle\mathcal{B},q\rangle=0$, significa que $\langle b,q\rangle = 0$ para todo $b\in\mathcal{B}$.

3.1.10 Teorema. Sea $\mathcal{A}$ una álgebra alternativa cuadrática. Si $\mathcal{B}$ es una subálgebra de $\mathcal{A}$ tal que $e\in\mathcal{B}$ y $q\in\mathcal{A}$ es tal que $\langle\mathcal{B},q\rangle=0$, entonces

1) $\langle\mathcal{B},\mathcal{B}q\rangle=0$, en particular $\mathcal{B}q\subset \mathrm{Im}\mathcal{A}$ y $\lambda\left(\mathcal{B}\cdot\mathcal{B}q\right)=0$.

2) Para $u,v\in\mathcal{B}$, se tiene

$$u\cdot vq = vu\cdot q, \tag{I}$$

$$uq \cdot v = u\overline{v} \cdot q, \text{ en particular } qv = \overline{v}q, \tag{II}$$

$$uq \cdot vq = -\langle q, q\rangle \cdot \overline{v}u. \tag{III}$$

3) $\mathcal{B} + \mathcal{B}q = \{u + vq\,; u, v \in \mathcal{B}\}$ es una subálgebra de $\mathcal{A}$.

Prueba. Como $e \in \mathcal{B}$, para todo $u \in \mathcal{B}$ se tiene $\overline{u} = 2\lambda(u)e - u$.

1) Dados $u, v \in \mathcal{B}$, se tiene

$$\begin{aligned} \langle u, vq\rangle &= \langle vq, u\rangle = \langle q, \overline{v}\, u\rangle \\ &= \langle \overline{v}\, u, q\rangle = 0 \end{aligned}$$

Es decir, $\langle \mathcal{B}, \mathcal{B}q\rangle = 0$. Ahora (3.1.1) garantiza que

$0 = \langle u, vq\rangle = 2\lambda(u)\lambda(vq) - \dfrac{1}{2}\lambda(u \cdot vq + vq \cdot u)$

$2\lambda(u)\lambda(vq) = \dfrac{1}{2}\lambda(u \cdot vq + vq \cdot u);\quad u, v \in \mathcal{B}$

$4\lambda(u)\lambda(vq) = \lambda(u \cdot vq + vq \cdot u)\,.$

Para $u = e$, se tiene $4\lambda(vq) = \lambda(vq + vq)$. Es decir, $2\lambda(vq) = 0$. En consecuencia, $\mathcal{B}q \subset \mathrm{Im}\mathcal{A}$.

Sean $u, v \in \mathcal{B}$. Como $\mathcal{A}$ es un álgebra alternativa cuadrática, por (1) de (3.1.4) se tiene $\langle u, vq\rangle = 2\lambda(u)\lambda(vq) - \lambda(u \cdot vq)$. Como $\langle u, vq\rangle = 0$ y $vq \in \mathcal{B}_q \subset \mathrm{Im}\mathcal{A}$, se concluye que $\lambda(u \cdot vq) = 0$. Por tanto, $\lambda\left(\mathcal{B} \cdot \mathcal{B}q\right) = 0$.

2) <u>Afirmación</u>.- Para todo $v \in \mathcal{B}$, se tiene

$$qv = \overline{v}\, q \tag{$*$}$$

En efecto:

- Si $v \in \mathbb{R}e$, es claro que $qv = \overline{v}\, q$.
- Si $v \in \mathrm{Im}\mathcal{B}$, entonces $vq + qv = 0$ (ver 3 de 3.1.6). Por otro lado como $e \in \mathcal{B}$ y $\overline{v} = 2\lambda(v)e - v$, $v = -\overline{v}$. Luego, $qv = -vq = \overline{v}\, q$.

Sean $u, v \in \mathcal{B}$.

<u>Caso 1</u>: $u \in \mathbb{R}e$ o $v \in \mathbb{R}e$.

Para fijar ideas, consideremos $u = \alpha e$.

I) $u \cdot vq = (\alpha e)vq = \alpha vq$; $vu \cdot q = v(\alpha e) \cdot q = \alpha vq$.

II) $uq\cdot v=(\alpha e)q\cdot v=\alpha qv$; $u\,\overline{v}\cdot q=(\alpha e)\overline{v}q=\alpha\,\overline{v}\,q=\alpha qv$ (ver $(*)$).

$$\begin{aligned}
\text{III) } uq\cdot vq &= (\alpha e)q\cdot vq=\alpha q\cdot\left(\overline{\overline{v}}\,q\right)=\alpha q\cdot q\,\overline{v} \quad (\text{ver } (*))\\
&= \alpha q^2\,\overline{v} \quad (\mathcal{A} \text{ es alternativa})\\
&= \alpha\left[2\lambda(q)q-\langle q,q\rangle e\right]\overline{v} \quad (\text{ver 3 de 3.1.1})\\
&= -\langle q,q\rangle\,\alpha\,\overline{v}=-\langle q,q\rangle\,\overline{v}\,u
\end{aligned}$$

<u>Caso 2</u>: $u,v\in \mathrm{Im}\mathcal{B}$.

$$\begin{aligned}
\text{I) } u\cdot vq-vu\cdot q &= u\cdot vq+uv\cdot q-vu\cdot q-uv\cdot q\\
&= u\cdot vq+uv\cdot q-(uv+vu)q\\
&= 2\lambda(vq)x-2\lambda(uq)y+2\lambda(uv)q+2\lambda(uv\cdot q)e-\\
&\quad\ (-2\langle u,v\rangle e) \quad (\text{ver 1 de 3.1.8 y 3.1.2})\\
&= 0 \quad (\text{ver 1 de 3.1.6})
\end{aligned}$$

II) De (3), $v\cdot uq=uv\cdot q$. Luego,

$\overline{v\cdot uq}=\overline{uv\cdot q}$

$\overline{uq}\cdot\overline{v}=\overline{q}\cdot\overline{uv}$

$\overline{q}\,\overline{u}\cdot\overline{v}=\overline{q}\cdot\overline{v}\,\overline{u}$

$qu\cdot v=q\cdot vu.$

Ahora aplicando $(*)$, se obtiene

$\overline{u}\,q\cdot v=\overline{vu}\cdot q$

$-\,uq\cdot v=-u\,\overline{v}\cdot q.$

Por tanto, $uq\cdot v=u\,\overline{v}\cdot q$. En particular, para $u=e$ se tiene $q\cdot v=\overline{v}\cdot q$.

$$\begin{aligned}
\text{III) De 1), } \lambda(vq\cdot q) &= \lambda(vq^2)\\
&= \lambda\left(v\left[2\lambda(q)q-\langle q,q\rangle e\right]\right) \quad (\text{ver 3 de 3.1.1})\\
&= -\langle q,q\rangle\,\lambda(v)=0
\end{aligned}$$

Es decir, u,q,vq son ortogonales dos a dos en $\mathrm{Im}\mathcal{A}$. Considerando $x=u,y=q$ y $z=vq$ en (3.1.9), se tiene

$$\begin{aligned}
(uq)\cdot(vq) &= (-vq)q\cdot u\\
&= -vq^2\cdot u\\
&= \left(-v\left[2\lambda(q)q-\langle q,q\rangle e\right]\right)\cdot u\\
&= -\langle q,q\rangle\,\overline{v}\,u.
\end{aligned}$$

En consecuencia, $uq\cdot vq=-\langle q,q\rangle\,\overline{v}\,u$.

3) Dados $u+vq,u_1+v_1q\in\mathcal{B}+\mathcal{B}q$, utilizando las relaciones (I), (II) y (III) se obtiene

$$\begin{aligned}(u+vq)(u_1+v_1q) &= (u+vq)u_1+(u+vq)v_1q\\ &= uu_1+vq\cdot u_1+u\cdot v_1q+vq\cdot v_1q\\ &= uu_1+v\,\overline{u_1}\cdot q+v_1u\cdot q-\langle q,q\rangle\,\overline{v_1}\,v\\ &= uu_1-\langle q,q\rangle\,\overline{v_1}\,v+(v\,\overline{u_1}+v_1u)\,q.\end{aligned}$$

Por tanto, $\mathcal{B}+\mathcal{B}q$ es una subálgebra de $\mathcal{A}$.■

3.1.11 Teorema. Sean $\mathcal{A}$ un álgebra alternativa, cuadrática sin divisores de cero y $\mathcal{B}$ una subálgebra propia de $\mathcal{A}$. Si $\mathcal{B}$ contiene al elemento unidad e de $\mathcal{A}$, entonces

1) Existe un elemento $q\in \mathrm{Im}\mathcal{A}$ tal que $q^2=-e$ y $\langle \mathcal{B},q\rangle=0$.

2) Para todo $q\in \mathrm{Im}\mathcal{A}$ con $q^2=-e$ y $\langle \mathcal{B},q\rangle=0$, el conjunto $\mathcal{B}+\mathcal{B}q$ es una subálgebra de $\mathcal{A}$ con $\dim(\mathcal{B}+\mathcal{B}q)=2\dim\mathcal{B}$ y para $u,v\in\mathcal{B}$ se tiene
   $u\cdot vq=vu\cdot q$, $uq\cdot v=u\,\overline{v}\cdot q$ en particular $qv=\overline{v}q$ y $uq\cdot vq=-\langle q,q\rangle\,\overline{v}u$.

3) $\mathcal{B}$ es asociativa.

Prueba.

1) Por (2.3.12), se tiene $\mathcal{A}=\mathbb{R}e\oplus\mathrm{Im}\mathcal{A}$ y $\mathcal{B}=\mathbb{R}e\oplus\mathrm{Im}\mathcal{B}$. Como $\mathcal{B}\neq\mathcal{A}$, existe $t\in\mathrm{Im}\mathcal{A}\setminus\mathcal{B}$ con $t\neq 0$. Ahora por (2.3.3), existe $w>0$ tal que $t^2=-we$. Por ende existe $q=\frac{t}{\sqrt{w}}\in\mathrm{Im}\mathcal{A}$ tal que $q^2=-e$.
   Sea $p\in\mathcal{B}$. Supongamos que existe $r\in\mathbb{R}\setminus\{0\}$ tal que $pq=re$. Como $\mathcal{A}$ es alternativa, $pq^2=rq$; contradiciendo que $q\notin\mathcal{B}$. Por tanto, $pq\notin\mathbb{R}e\setminus\{0\}$.
   Si $\lambda(pq)\neq 0$, existe $\rho\in\mathbb{R}$ tal que $pq=\rho e$. En consecuencia, $\lambda(pq)=0$. Finalmente el corolario (3.1.6) garantiza que $\langle\mathcal{B},q\rangle=0$.

2) Elijamos $q\in\mathrm{Im}\mathcal{A}$ tal que $q^2=-e$ y $\langle\mathcal{B},q\rangle=0$. Por (c) de (3.1.10), $\mathcal{B}+\mathcal{B}q$ es una subálgebra de $\mathcal{A}$ y por (a) de (3.1.10) se tiene que esta suma es directa. Como $\mathcal{A}$ es alternativa, $vq\cdot q=-v$. En consecuencia la aplicación, $v\mapsto vq$ de $\mathcal{B}$ sobre $\mathcal{B}q$ es inyectiva. Además, $\langle\mathcal{B},\mathcal{B}q\rangle=0$.

3) Sean $u,v,w\in\mathcal{B}$. Por (3) de (3.1.10), se tiene

$$(uv\cdot w)q=w(uv\cdot q)=w(v\cdot uq) \qquad (*)$$

Es claro que $\langle \mathcal{B}, uq\rangle = 0$, pues $\langle \mathcal{B}, \mathcal{B}q\rangle = 0$. Así la expresión (3) de (3.1.10) es válida para q y uq. Luego

$$(u \cdot vw)q = vw \cdot uq = w(v \cdot uq) \qquad (**)$$

Finalmente de $(*)$ y $(**)$, se concluye que $uv \cdot w = u \cdot vw$.■

3.2. El álgebra de los Octoniones $\mathbb{O}$

3.2.1 Definición. Dados $x = (x_1, x_2), y = (y_1, y_2) \in \mathbb{H} \times \mathbb{H}$ definimos el producto xy como $xy = (x_1, x_2)(y_1, y_2) = (x_1y_1 - \overline{y_2}x_2, x_2\overline{y_1} + y_2x_1)$.

Dados $\alpha, \beta \in \mathbb{R}$ y $x = (x_1, x_2), y = (y_1, y_2), z = (z_1, z_2) \in \mathbb{H} \times \mathbb{H}$, y considerando que $\mathbb{H}$ es un $\mathbb{R}$-álgebra, se tiene

$$\begin{aligned}
(\alpha x + \beta y)z &= [\,(\alpha x_1, \alpha x_2) + (\beta y_1, \beta y_2)\,]\,(z_1, z_2) \\
&= (\alpha x_1 + \beta y_1, \alpha x_2 + \beta y_2)\,(z_1, z_2) \\
&= (\,[\alpha x_1 + \beta y_1]\,z_1 - \overline{z_2}\,[\alpha x_2 + \beta y_2]\,, [\alpha x_2 + \beta y_2]\,\overline{z_1} + z_2\,[\alpha x_1 + \beta y_1]\,) \\
&= (\alpha x_1 z_1 + \beta y_1 z_1 - \alpha\overline{z_2}\,x_2 - \beta\,\overline{z_2}\,y_2\,,\, \alpha x_2\overline{z_1} + \beta y_2\overline{z_1} + \alpha z_2 x_1 + \beta z_2 y_1) \\
&= (\alpha x_1 z_1 - \alpha\overline{z_2}\,x_2 + \beta y_1 z_1 - \beta\,\overline{z_2}\,y_2\,,\, \alpha x_2\overline{z_1} + \alpha z_2 x_1 + \beta y_2\overline{z_1} + \beta z_2 y_1) \\
&= (\alpha x_1 z_1 - \alpha\overline{z_2}x_2\,,\, \alpha x_2\overline{z_1} + \alpha z_2 x_1) + (\beta y_1 z_1 - \beta\,\overline{z_2}y_2\,,\, \beta y_2\overline{z_1} + \beta z_2 y_1) \\
&= \alpha\,(x_1 z_1 - \overline{z_2}\,x_2\,,\, x_2\,\overline{z_1} + z_2 x_1) + \beta\,(y_1 z_1 - \overline{z_2}\,y_2\,,\, y_2\,\overline{z_1} + z_2 y_1) \\
&= \alpha xz + \beta yz
\end{aligned}$$

Analogamente se verifica que $x\,(\alpha y + \beta z) = \alpha xy + \beta xz$. En consecuencia, $\mathbb{H} \times \mathbb{H}$ es un $\mathbb{R}$-álgebra de dimensión 8 llamada álgebra de Cayley de los Octoniones y se denota por $\mathbb{O}$.

Denotemos con $\hat{e}$ a la unidad de $\mathbb{H}$. Si $e = (\hat{e}, 0) \in \mathbb{H} \times \mathbb{H}$, entonces $ex = x$ y $xe = x$ para todo $x \in \mathbb{O}$. Es decir, $e = (\hat{e}, 0)$ es el elemento unidad de $\mathbb{O}$.

3.2.2 Teorema. Si $x = (x_1, x_2) \in \mathbb{O}$, entonces

$$x^2 = 2\mathrm{Re}(x_1)x - (\langle x_1, x_1\rangle + \langle x_2, x_2\rangle)\,e.$$

Prueba. $x^2 = (x_1, x_2)(x_1, x_2) = (x_1^2 - \overline{x_2}x_2, x_2\overline{x_1} + x_2x_1)\,.$

Como $x_1, x_2 \in \mathbb{H}$, de 2.2.10 se tiene

$$x_1^2 = 2\mathrm{Re}(x_1)x_1 - \langle x_1, x_1\rangle\,\hat{e}, \quad \overline{x_2}x_2 = \langle x_2, x_2\rangle\,\hat{e} \quad \text{y} \quad \overline{x_1} + x_1 = 2\mathrm{Re}(x_1)\hat{e}.$$

Ahora,

$$\begin{aligned}
x^2 &= (2\mathrm{Re}(x_1)x_1 - \langle x_1, x_1\rangle\,\hat{e} - \langle x_2, x_2\rangle\,\hat{e}, x_2(\overline{x_1} + x_1)) \\
&= (2\mathrm{Re}(x_1)x_1 - [\langle x_1, x_1\rangle + \langle x_2, x_2\rangle]\,\hat{e}, 2\mathrm{Re}(x_1)x_2) \\
&= (2\mathrm{Re}(x_1)x_1, 2\mathrm{Re}(x_1)x_2) + (-[\langle x_1, x_1\rangle + \langle x_2, x_2\rangle]\,\hat{e}, 0) \\
&= 2\mathrm{Re}(x_1)(x_1, x_2) - (\langle x_1, x_1\rangle + \langle x_2, x_2\rangle)\,(\hat{e}, 0)
\end{aligned}$$

Por lo tanto, $x^2 = 2\mathrm{Re}(x_1)x - (\langle x_1, x_1\rangle + \langle x_2, x_2\rangle)\,e.$■

Como $\mathbb{O}$ es cuadrática, $\mathbb{O} = \mathbb{R}e \oplus \mathrm{Im}\mathbb{O}$. La forma $\mathbb{R}$-lineal λ, la forma bilineal $\langle\,,\rangle$ y la aplicación conjugación $x \mapsto \overline{x}$ se definen como en la sección **2.1**. Las relaciones en 3.1.1 y la definición 2.2.9, nos permiten reescribir estás definiciones como

3.2.3 Definición. Dados $x = (x_1, x_2), y = (y_1, y_1) \in \mathbb{O}$, se define

1. $\lambda : \mathbb{O} \to \mathbb{R}$ como $\lambda(x) = \mathrm{Re}(x_1)$
2. $\langle\,,\rangle : \mathbb{O} \times \mathbb{O} \to \mathbb{R}$ por $\langle x, y\rangle = \langle x_1, y_1\rangle + \langle x_2, y_2\rangle$
3. $\mathrm{Im}\mathbb{O} = \mathrm{Im}\mathbb{H} \times \mathbb{H}$
4. $^{-} : \mathbb{O} \to \mathbb{O}$ como $\overline{x} = (\overline{x_1}, -x_2)$

Note que la forma bilineal de $\mathbb{O}$ es definida positiva, pues la forma bilineal $\langle\,,\rangle$ de $\mathbb{H}$ lo es.

3.2.4 Teorema. Si $x, y \in \mathbb{O}$, entonces

1. $\overline{x\,y} = \overline{y}\,\overline{x}$
2. $x\,\overline{x} = \overline{x}\,x = \langle x, x\rangle\, e$
3. $x\,(\overline{x}\,y) = \langle x, x\rangle\, y = (x\,\overline{x})\,y$

Prueba. Sean $x = (x_1, x_2), y = (y_1, y_2) \in \mathbb{O}$.

1. $$\begin{aligned}
\overline{x\,y} &= \big(\overline{x_1y_1 - \overline{y_2}x_2}, -x_2\,\overline{y_1} - y_2x_1\big) \\
&= \big(\overline{x_1y_1} - \overline{\overline{y_2}\,x_2}, -x_2\,\overline{y_1} - y_2x_1\big) \\
&= (\,\overline{y_1}\,\overline{x_1} - \overline{x_2}\,y_2, -x_2\,\overline{y_1} - y_2x_1) \quad \text{(ver 2 de 2.2.10).}
\end{aligned}$$

$$\begin{aligned}\overline{y}\,\overline{x} &= (\,\overline{y_1}, -y_2)\,(\,\overline{x_1}, -x_2) \\ &= (\,\overline{y_1}\,\overline{x_1} - \overline{x_2}\,y_2, -y_2x_1 - x_2\,\overline{y_1})\end{aligned}$$

En consecuencia, $\overline{xy} = \overline{y}\,\overline{x}$.

2. $$\begin{aligned} x\overline{x} &= (x_1, x_2)(\overline{x_1}, -x_2) = \Big(x_1\overline{x_1} - \overline{(-x_2)}x_2, x_2\overline{\overline{x_1}} + (-x_2)x_1\Big) \\ &= (x_1\overline{x_1} + \overline{x_2}x_2, x_2x_1 - x_2x_1) = (x_1\overline{x_1} + \overline{x_2}x_2, 0) \end{aligned}$$

$$\begin{aligned} \overline{x}x &= (\overline{x_1}, -x_2)(x_1, x_2) = (\overline{x_1}x_1 - \overline{x_2}(-x_2), -x_2\overline{x_1} + x_2\overline{x_1}) \\ &= (x_1\overline{x_1} + \overline{x_2}x_2, 0) \quad \text{(ver 4 de 2.2.10)} \end{aligned}$$

$$\begin{aligned} \overline{x}x &= (\langle x_1, x_1\rangle\,\hat{e} + \langle x_2, x_2\rangle\,\hat{e}, 0) \quad \text{(ver 4 de 2.2.10)} \\ &= (\langle x_1, x_1\rangle + \langle x_2, x_2\rangle)\,(\hat{e}, 0) = \langle x, x\rangle\,e \end{aligned}$$

Por tanto, $x\overline{x} = \overline{x}x = \langle x, x\rangle\,e$.

3. $\overline{x}y = (\overline{x_1}, -x_2)(y_1, y_2) = (\overline{x_1}y_1 - y_2(-x_2), -x_2\overline{y_1} + y_2\overline{x_1})$. Como el álgebra $\mathbb{H}$ es asociativa, se tiene

$$\begin{aligned} \cdot\ x(\overline{x}y) &= (x_1[\,\overline{x_1}y_1 + \overline{y_2}x_2\,] - [-y_1\overline{x_2} + x_1\overline{y_2}\,]x_2, x_2[\,\overline{y_1}x_1 + \overline{x_2}y_2\,] + \cdots \\ &\qquad \cdots + [-x_2\overline{y_1} + y_2\overline{x_1}\,]x_1) \\ &= (x_1\overline{x_1}y_1 + y_1\overline{x_2}x_2, x_2\overline{x_2}y_2 - y_2\overline{x_1}x_1) \\ &= (\langle x_1, x_1\rangle\,y_1 + \langle x_2, x_2\rangle\,y_1, \langle x_2, x_2\rangle\,y_2 + \langle x_1, x_1\rangle\,y_2) \quad \text{(ver 4 de 2.2.10)} \\ &= (\langle x_1, x_1\rangle + \langle x_2, x_2\rangle)\,(y_1, y_2) = \langle x, x\rangle\,y. \end{aligned}$$

$$\begin{aligned} \cdot\ (x\overline{x})y &= (x_1\overline{x_1} + \overline{x_2}x_2, 0) \\ &= ([\,x_1\overline{x_1} + \overline{x_2}x_2\,], y_2[\,x_1\overline{x_1} + \overline{x_2}x_2]) \\ &= ([\langle x_1, x_1\rangle + \langle x_2, x_2\rangle]y_1, [\langle x_1, x_1\rangle + \langle x_2, x_2\rangle]y_2) = \langle x, x\rangle\,y. \end{aligned}$$

Por lo tanto, $x(\overline{x}y) = \langle x, x\rangle\,y = (x\overline{x})y.$■

3.2.5 Teorema. El álgebra $\mathbb{O}$ es un álgebra alternativa de división.

Prueba. Sean $x, y \in \mathbb{O}$. Como $\mathbb{O}$ es un $\mathbb{R}$-álgebra cuadrática, se tiene $\overline{x} = 2\lambda(x)e - x$. Ahora por (3) de (3.2.4), $x(\overline{x}y) = (x\,\overline{x})y$.

$$x\left([2\lambda(x)e - x]y\right) = \left(x[2\lambda(x)e - x]\right)y$$

$$x\left(2\lambda(x)y - xy\right) = \left(2\lambda(x)x - x^2\right)y$$

$$2\lambda(x)xy - x(xy) = 2\lambda(x)xy - x^2y$$

$$x(xy) = x^2y$$

Por otro lado,

$$\overline{x(xy)} = \overline{x^2 y}$$
$$(\overline{xy})\,\overline{x} = \overline{y}\,\overline{x^2}$$
$$(\overline{y}\,\overline{x})\,\overline{x} = \overline{y}\,\overline{x}^2.$$

Como $\overline{x}, \overline{y}$ varian en todo $\mathbb{O}$ cuando x, y recorren $\mathbb{O}$, se concluye que $(yx)\,x = yx^2$. Por tanto, $\mathbb{O}$ es un álgebra alternativa. Como la forma bilineal de $\mathbb{O}$ es definida positiva, (1) de (3.1.5) garantiza que $\mathbb{O}$ no tiene divisores de cero. Por lo tanto, $\mathbb{O}$ es un álgebra de división (ver 1.1.12).■

3.2.6 Nota. Se tiene

1. Como $\mathbb{O}$ es un $\mathbb{R}$-álgebra cuadrática sin divisores de cero, el teorema de Frobenius garantiza que $\mathbb{O}$ es un álgebra no asociativa.

2. Si $\mathbb{R}$ en $\mathbb{C}$ es identificado con los pares $(\alpha, 0)$, $\alpha \in \mathbb{R}$ y $\mathbb{C}$ en $\mathbb{H}$ es identificado con los cuaterniones $(\alpha, \beta, 0, 0)$, $\alpha, \beta \in \mathbb{R}$, las álgebras $\mathbb{C}$ y $\mathbb{H}$ tienen las representaciones $\mathbb{C} = \mathbb{R} \oplus \mathbb{R}i$ y $\mathbb{H} = \mathbb{C} \oplus \mathbb{C}j$ respectivamente como suma directa de $\mathbb{R}$-espacios vectoriales. En este sentido, $\mathbb{R}$ es una subálgebra de $\mathbb{C}$ conteniendo al elemento identidad de $\mathbb{C}$ y $\mathbb{C}$ es una subálgebra de $\mathbb{H}$ que contiene al elemento identidad de $\mathbb{H}$.

3. El conjunto $\{(u, 0); u \in \mathbb{H}\}$ es una subálgebra de $\mathbb{O}$, isomorfa al álgebra de los cuaterniones $\mathbb{H}$ y contiene al elemento unidad e de $\mathbb{O}$. Identificamos está subálgebra con $\mathbb{H}$ y las siguientes reglas de multiplicación son válidas para todo $u \in \mathbb{H}$ y todo $(a_1, a_2) \in \mathbb{O}$: $u(a_1, a_2) = (ua_1, ua_2)$, $(a_1, a_2)u = (a_1 u, a_2\,\overline{u})$. Si $p = (0, \hat{e})$, entonces $p^2 = -e$, $(a_1, a_2) = a_1 + a_2 p$ para todo $(a_1, a_2) \in \mathbb{O}$.

3.2.7 Teorema. Si consideramos $\mathbb{O}$ como $\mathbb{R}$-espacio vectorial, $\mathbb{O} = \mathbb{H} \oplus \mathbb{H}p$. Está suma es ortogonal con respecto al producto interno de $\mathbb{O}$. Para todo $u, v \in \mathbb{H}$ se verifica

1. $u(vp) = (vu)p$

2. $(up)v = (u\,\overline{v})p$, en particular $pv = \overline{v}p$

3. $(up)(vp) = -\overline{v}u$

Prueba. Dado $(a_1, a_2) \in \mathbb{O}$, se tiene $(a_1, a_2) = a_1e + a_2p$. Es decir, $\mathbb{O} = \mathbb{H} + \mathbb{H}p$. Como

$$\langle a_1e, a_2p\rangle = \langle (a_1, 0), (0, a_2)\rangle = \langle a_1, 0\rangle + \langle 0, a_2\rangle = 0$$

esta representación es ortogonal y en consecuencia la suma es directa. Ahora dados $u, v \in \mathbb{H}$, se tiene

1) $u(vp) = u(0, v) = (0, vu) = (vu)p$

2) $(up)v = (0, u)v = (0, u\,\overline{v}) = (u\,\overline{v})p$

   En particular, $u = \hat{e} \Rightarrow pv = \overline{v}p$.

3) $(up)(vp) = (0, u)(0, v) = (-\overline{v}u, 0) = -\overline{v}u.$ ■

3.2.8 Nota. En $V = \mathbb{R}^8$ consideremos la base canónica

$$e_1 = (1, 0, \ldots, 0),\ e_2 = (0, 1, \ldots, 0), \ldots, e_8 = (0, \ldots, 0, 1).$$

La tabla de multiplicación para $\mathbb{O}$ es

$\cdot$	e_2	e_3	e_4	e_5	e_6	e_7	e_8
e_2	$-e_1$	e_4	$-e_3$	e_6	$-e_5$	$-e_8$	e_7
e_3	$-e_4$	$-e_1$	e_2	e_7	e_8	$-e_5$	$-e_6$
e_4	e_3	$-e_2$	$-e_1$	e_8	$-e_7$	e_6	$-e_5$
e_5	$-e_6$	$-e_7$	$-e_8$	$-e_1$	e_2	e_3	e_4
e_6	e_5	$-e_8$	e_7	$-e_2$	$-e_1$	$-e_4$	e_3
e_7	e_8	e_5	$-e_6$	$-e_3$	e_4	$-e_1$	$-e_2$
e_8	$-e_7$	e_6	e_5	$-e_4$	$-e_3$	e_2	$-e_1$

3.2.9 Teorema (Unicidad de los Octoniones)**.** Sea $\mathcal{A}$ un $\mathbb{R}$-álgebra alternativa, cuadrática sin divisores de cero. Si $\mathcal{A}$ no es asociativa, entonces $\mathcal{A}$ es isomorfa al álgebra de Cayley $\mathbb{O}$.

Prueba. Es claro que $\dim\mathcal{A} \geq 2$. Por otro lado, como $\mathcal{A}$ es cuadrática y sin divisores de cero, $\mathcal{A} = \mathbb{R}e \oplus \mathrm{Im}\mathcal{A}$ y existe $q \in \mathrm{Im}\mathcal{A}$ tal que $q^2 = -e$. Si $\dim\mathcal{A} = 2$, la aplicación $\mathbb{C} \to \mathcal{A}$, $a + bi \mapsto ae + bq$ es un isomorfismo de $\mathbb{R}$-álgebras. Por ende, $\dim\mathcal{A} \geq 3$. Si $\dim\mathcal{A} \geq 3$, (2.3.14) garantiza que existe $\mathcal{B}$ subálgebra de $\mathcal{A}$ con $e \in \mathcal{B}$ y un isomorfismo $f : \mathbb{H} \to \mathcal{B}$. Como $\mathcal{A}$ es no asociativa, $\mathcal{B} \neq \mathcal{A}$. Por (1) y (2) de (3.1.11), existe $q \in \mathcal{A}$ tal que $q^2 = -e$, $\langle \mathcal{B}, q \rangle = 0$ y $\mathcal{B} \oplus \mathcal{B}q$ es una subálgebra de $\mathcal{A}$ que contiene a e.

Como $\mathbb{O} = \mathbb{H}e \oplus \mathbb{H}p$ (ver 3.2.7), definamos la aplicación $\xi : \mathbb{H}e \oplus \mathbb{H}p \to \mathcal{B} \oplus \mathcal{B}q$ por $\xi(ue + vp) = f(u) + f(v)q$.

Si $\xi(ue + vp) = \xi(u_1e + v_1p)$, se tiene

$f(u) + f(v)q = f(u_1) + f(v_1)q$

$f(u) + f(v)f(p) = f(u_1) + f(v_1)f(p)$

$f(u + vp) = f(u_1 + v_1p)$

$u + vp = u_1 + v_1p$

y como $\mathbb{H}e \cap \mathbb{H}p = \{0\}$, se concluye que $u = u_1$ y $v = v_1$.

Por otro lado, dado $w \in \mathcal{B} \oplus \mathcal{B}q$, existen $u_1, v_1 \in \mathcal{B}$ tales que $w = u_1 + v_1q$. La sobreyectividad de $f : \mathbb{H} \to \mathcal{B}$ garantiza la existencia de $u, v \in \mathbb{H}$ tales que $f(u) = u_1$ y $f(v) = v_1$. Es decir, existe $a = u + vp \in \mathbb{H}e \oplus \mathbb{H}p$ tal que $\xi(a) = w$.

Dados $x = ue + vp, y = ae + bp \in \mathbb{O}$, considerando (3.2.7) se obtiene

$$\begin{aligned}
\xi(xy) &= \xi\left((ue + vp)(ae + bp)\right) \\
&= \xi\left((ue)(ae) + (ue)(bp) + (vp)(ae) + (vp)(bp)\right) \\
&= \xi\left((ua)e + u(bp) + (vp)a + (-\overline{b})\,v\right) \\
&= \xi\left((ua)e + (bu)p + (v\,\overline{a})p + (-\overline{b}\,v)e\right) \\
&= \xi\left((ua + (-\overline{b}\,)v)e + (bu + v\,\overline{a})p\right) \\
&= f\left(ua - \overline{b}\,v\right) + f\left(bu + v\,\overline{a}\right)q \\
&= f(ua) - f(\overline{b}\,v) + f(bu)q + f(v\,\overline{a})q
\end{aligned}$$

Ahora de (3.1.10) obtenemos

$$
\begin{aligned}
\xi(x)\xi(y) &= \xi(ue+vp)\xi(ae+bp)\\
&= (f(u)+f(v)q)\,(f(a)+f(b)q)\\
&= f(u)f(a)+f(u)\,(f(b)q)+(f(v)q)\,f(a)+(f(v)q)\,(f(b)q)\\
&= f(ua)+(f(b)f(u))\,q+\Big(f(v)\,\overline{f(a)}\Big)\,q+\Big(-\langle q,q\rangle\,\overline{f(b)}f(v)\Big)\\
&= f(ua)+f(bu)q+f(v\,\overline{a})q-f\left(\overline{b}\,v\right)
\end{aligned}
$$

Es decir, $\xi(xy)=\xi(x)\xi(y)$ para todo $x,y\in\mathbb{O}$.

Note que $e=e+0q\in\mathcal{B}\oplus\mathcal{B}q$. Si $\mathcal{B}\oplus\mathcal{B}q\subsetneq\mathcal{A}$, $\mathcal{B}\oplus\mathcal{B}q$ es asociativa (ver 3 de 3.1.11) contradiciendo la no asociatividad de $\mathbb{O}$. Por lo tanto, $\mathcal{B}\oplus\mathcal{B}q=\mathcal{A}$.$\blacksquare$

3.3. Una representación matricial de los Octoniones

Dados $x=(x_1,x_2), y=(y_1,y_2)\in\mathbb{O}$, se tiene

$$xy=(x_1,x_2)(y_1,y_2)=(x_1y_1-\overline{y_2}\,x_2,x_2\,\overline{y_1}+y_2x_1)$$

donde $x_1=\alpha_1e+u_1$, $x_2=\alpha_2e+u_2$, $y_1=\beta_1e+v_1$, $y_2=\beta_2e+v_2\in\mathbb{H}=\mathbb{R}e\oplus\mathrm{Im}\mathbb{H}$. Considerando (6) de (2.2.10), se tiene

$u_1v_1=-\langle u_1,v_1\rangle\,e+u_1\times v_1\,,\quad v_2u_2=-\langle v_2,u_2\rangle\,e+v_2\times u_2\,,$

$u_2v_1=-\langle u_2,v_1\rangle\,e+u_2\times v_1\quad$ y $\quad v_2u_1=-\langle v_2,u_1\rangle\,e+v_2\times u_1.$

Utilizando estas expresiones y teniendo en cuenta que $\mathbb{H}$ es un $\mathbb{R}-$álgebra, podemos reescribir xy en la forma

$$
\begin{aligned}
xy=\big([\alpha_1\beta_1-\alpha_2\beta_2-\langle u_1,v_1\rangle-\langle u_2,v_2\rangle]e+\alpha_1v_1+\beta_1u_1-\beta_2u_2\\
+\alpha_2v_2+u_1\times v_1-u_2\times v_2\,,[\alpha_2\beta_1+\alpha_1\beta_2+\langle u_2,v_1\rangle-\langle u_1,v_2\rangle]e\\
-\alpha_2v_1+\beta_2u_1+\alpha_1v_2+\beta_1u_2-u_2\times v_1-u_1\times v_2\big)\quad \text{(I)}
\end{aligned}
$$

Consideremos u_1,u_2,v_1 y v_2 como vectores de $\mathbb{R}^3$ y definamos

$$\alpha=\alpha_1+i\alpha_2,\beta=\beta_1+i\beta_2\in\mathbb{C}\quad\text{y}\quad u=u_1+iu_2,v=v_1+iv_2\in\mathbb{C}^3\qquad\text{(II)}$$

De ahora en adelante una barra será usada solo para la conjugación compleja. Para los vectores $z = (z_1, z_2, z_3), w = (w_1, w_2, w_3) \in \mathbb{C}^3$, definimos

$$\langle z, w\rangle = \sum_{\mu=1}^{3} z_\mu w_\mu \quad \text{y} \quad z \times w = (z_2w_3 - z_3w_2, z_3w_1 - z_1w_3, z_1w_2 - z_2w_1).$$

Utilizando estas expresiones obtenemos

$\alpha\beta = \alpha_1\beta_1 - \alpha_2\beta_2 + (\alpha_1\beta_2 + \alpha_2\beta_1)i\,,$

$\langle\overline{u}, v\rangle = \langle u_1, v_1\rangle + \langle u_2, v_2\rangle + (\langle u_1, v_2\rangle - \langle u_2, v_1\rangle)\,i\,,$

$\overline{\alpha}v = \alpha_1v_1 + \alpha_2v_2 + (\alpha_1v_2 - \alpha_2v_1)\,i\,,$

$\beta u = \beta_1u_1 - \beta_2u_2 + (\beta_2u_1 + \beta_1u_2)\,i$ y

$\overline{u} \times \overline{v} = u_1 \times v_1 - u_2 \times v_2 + (-u_2 \times v_1 - u_1 \times v_2)\,i$

Ahora reescribimos la expresión (I) como

$$\begin{aligned} xy = \big(&\mathrm{Re}\,([\alpha\beta - \langle\overline{u}, v\rangle]e + \overline{\alpha}v + \beta u + \overline{u} \times \overline{v})\,,\\ &\mathrm{Im}\,([\alpha\beta - \langle\overline{u}, v\rangle]e + \overline{\alpha}\,v + \beta u + \overline{u} \times \overline{v})\big) \end{aligned} \tag{III}$$

Ahora consideremos el $\mathbb{R}$-espacio vectorial de dimensión 8, $\mathfrak{C} = \mathbb{C}e \oplus \mathbb{C}^3$ con elementos $\alpha e + u$, $\alpha \in \mathbb{C}$ y $u \in \mathbb{C}^3$. Definamos $F : \mathbb{O} \to \mathfrak{C}$ por

$$F(x) = F(x_1, x_2) = F(\alpha_1e + u_1, \alpha_2e + u_2) = \alpha e + u = x_1 + ix_2 \tag{IV}$$

donde $\alpha = \alpha_1 + i\alpha_2$ y $u = u_1 + iu_2$.

Dados $x = (x_1, x_2), y = (y_1, y_2) \in \mathbb{O}$, utilizando (II) y (III) se tiene

$$\begin{aligned} F(xy) = F\big(&[\alpha_1\beta_1 - \alpha_2\beta_2 - \langle u_1, v_1\rangle - \langle u_2, v_2\rangle]e + \alpha_1v_1 + \beta_1u_1 - \beta_2u_2\\ &+ \alpha_2v_2 + u_1 \times v_1 - u_2 \times v_2\,, [\alpha_2\beta_1 + \alpha_1\beta_2 + \langle u_2, v_1\rangle - \langle u_1, v_2\rangle]e\\ &- \alpha_2v_1 + \beta_2u_1 + \alpha_1v_2 + \beta_1u_2 - u_2 \times v_1 - u_1 \times v_2\big) \end{aligned}$$

$$\begin{aligned} F(xy) &= [\alpha_1\beta_1 - \alpha_2\beta_2 - \langle u_1, v_1\rangle - \langle u_2, v_2\rangle + i\alpha_2\beta_1 + i\alpha_1\beta_2 + i\,\langle u_2, v_1\rangle\\ &- i\,\langle u_1, v_2\rangle]e + \alpha_1v_1 + \beta_1u_1 - \beta_2u_2 + \alpha_2v_2 + u_1 \times v_1 - u_2 \times v_2 - i\alpha_2v_1\\ &+ i\beta_2u_1 + i\alpha_1v_2 + i\beta_1u_2 - i\,u_2 \times v_1 - i\,u_1 \times v_2\\ &= [\alpha\beta - \langle\,\overline{u}, v\rangle]e + \overline{\alpha}\,v + \beta u + \overline{u} \times \overline{v}. \end{aligned} \tag{V}$$

El resultado en (V) nos suguiere definir la multiplicación en $\mathfrak{C}$ como

$$(\alpha e + u)(\beta e + v) = [\alpha\beta - \langle\,\overline{u}, v\rangle]e + \overline{\alpha}\,v + \beta u + \overline{u} \times \overline{v} \tag{VI}$$

Sean $x = \alpha e + u, y = \beta e + v, z = \gamma e + w \in \mathfrak{C}$ y $a, b \in \mathbb{R}$ cualesquiera.

- $(ax+by)z = [\alpha a e + au + b\beta e + bv]\,(\gamma e + w) = [(a\alpha + b\beta)e + au + bv]\,(\gamma e + w)$

  $= [(a\alpha + b\beta)\gamma - < a\overline{u} + b\overline{v} + w >]\, e + (a\overline{\alpha} + b\overline{\beta})w + \gamma(au + bv) + (a\overline{u} + b\overline{v}) \times \overline{w}$

  $= a\,[\alpha\gamma - \langle \overline{u}, w\rangle]\, e + b\,[\beta\gamma - \langle \overline{v}, w\rangle]\, e + a\overline{\alpha}w + b\overline{\beta}w + a\gamma u + b\gamma v + a\overline{u} \times \overline{w} + b\overline{v} \times \overline{w}$

- $axz + byz = a(\alpha e + u)(\gamma e + w) + b(\beta e + v)(\gamma e + w)$

  $= a([\alpha\gamma - < \overline{u}, w >]\, e + \overline{\alpha}w + \gamma u + \overline{u} \times \overline{w}) + b([\beta\gamma - < \overline{v}, w >]\, e + \overline{\beta}w + \gamma v + \overline{v} \times \overline{w})$

De estas dos expresiones se concluye que $(ax + by)z = a(xz) + b(yz)$. Procediendo similarmente obtenemos $x(ay + bz) = a(xy) + b(xz)$. En consecuencia, $\mathfrak{C}$ con el producto definido en (VI) es un $\mathbb{R}$-álgebra.

Ahora dados $x = (x_1, x_2), y = (y_1, y_2) \in \mathbb{O}$, de (IV) se tiene $F(x) = \alpha e + u$ y $F(y) = \beta e + v$. De las expresiones (V) y (VI), se concluye que

$F(xy) = [\alpha\beta - \langle \overline{u}, v\rangle]\, e + \overline{\alpha}v + \beta u + \overline{u} \times \overline{v} = (\alpha e + u)(\beta e + v) = F(x)F(y)$.

Por ende, la aplicación $F : \mathbb{O} \to \mathfrak{C}$ es un isomorfismo de $\mathbb{R}$-álgebras.

Ahora consideremos el conjunto $\mathfrak{M}$ de las matrices $\begin{pmatrix} \alpha & u \\ -\overline{u} & \overline{\alpha} \end{pmatrix}$, donde $\alpha \in \mathbb{C}$ y $u \in \mathbb{C}^3$.

La expresión (VI) nos motiva para definir la multiplicación en $\mathfrak{M}$ como

$$\begin{pmatrix} \alpha & u \\ -\overline{u} & \overline{\alpha} \end{pmatrix} \begin{pmatrix} \beta & v \\ -\overline{v} & \overline{\beta} \end{pmatrix} = \begin{pmatrix} \alpha\beta - \langle \overline{u}, v\rangle & \overline{\alpha}v + \beta u + \overline{u} \times \overline{v} \\ -\alpha\overline{v} - \overline{\beta}\,\overline{u} - u \times v & \overline{\alpha}\,\overline{\beta} - \langle u, \overline{v}\rangle \end{pmatrix} \tag{VII}$$

Sean $x = \begin{pmatrix} \alpha & u \\ -\overline{u} & \overline{\alpha} \end{pmatrix}, y = \begin{pmatrix} \beta & v \\ -\overline{v} & \overline{\beta} \end{pmatrix}, z = \begin{pmatrix} \gamma & w \\ -\overline{w} & \overline{\gamma} \end{pmatrix} \in \mathfrak{M}$ y $a, b \in \mathbb{R}$ cualesquiera.

Ahora teniendo presente (VII),

$$(ax + by)z = \begin{pmatrix} a\alpha + b\beta & au + bv \\ -a\overline{u} - b\overline{v} & a\overline{\alpha} + b\overline{\beta} \end{pmatrix} \begin{pmatrix} \gamma & w \\ -\overline{w} & \overline{\gamma} \end{pmatrix} =$$

$$= \begin{pmatrix} (a\alpha + b\beta)\gamma - \langle a\overline{u} + b\overline{v}, w\rangle & (a\overline{\alpha} + b\overline{\beta})w + \gamma(au + bv) + (a\overline{u} + b\overline{v}) \times \overline{w} \\ -(a\alpha + b\beta)\overline{w} - \overline{\gamma}(a\overline{u} + b\overline{v}) - (au + bv) \times w & (a\overline{\alpha} + b\overline{\beta})\overline{\gamma} - \langle au + bv, \overline{w}\rangle \end{pmatrix}$$

$$= \begin{pmatrix} a(\alpha\gamma - \langle \overline{u}, w\rangle) + b\,(\beta\gamma - \langle \overline{v}, w\rangle) & a(\overline{\alpha}w + \gamma u + \overline{u} \times \overline{w}) + b\,(\overline{\beta}w + \gamma v + \overline{v} \times \overline{w}) \\ a\,(-\alpha\overline{w} - \overline{\gamma}\,\overline{u} - u \times w) + b\,(-\beta\overline{w} - \overline{\gamma}\,\overline{v} - v \times w) & a\,(\overline{\alpha}\,\overline{\gamma} - \langle u, \overline{w}\rangle) + b\,(\overline{\beta}\,\overline{\gamma} - \langle v, \overline{w}\rangle) \end{pmatrix}$$

$$= \begin{pmatrix} a\,(\alpha\gamma - \langle \overline{u}, w\rangle) & a\,(\overline{\alpha}w + \gamma u + \overline{u} \times \overline{w}) \\ a\,(-\alpha\,\overline{w} - \overline{\gamma}\,\overline{u} - u \times w) & a\,(\overline{\alpha}\,\overline{\gamma} - \langle u, \overline{w}\rangle) \end{pmatrix} +$$

$$\begin{pmatrix} b\,(\beta\gamma - \langle \overline{v}, w\rangle) & b\left(\overline{\beta} w + \gamma v + \overline{v} \times \overline{w}\right) \\ b\,(-\beta\overline{w} - \overline{\gamma v} - v \times w) & b\left(\overline{\beta}\,\overline{\gamma} - \langle v, \overline{w}\rangle\right) \end{pmatrix}$$

$$= a\begin{pmatrix} \alpha & u \\ -\overline{u} & \overline{\alpha} \end{pmatrix}\begin{pmatrix} \gamma & w \\ -\overline{w} & \overline{\gamma} \end{pmatrix} + b\begin{pmatrix} \beta & v \\ -\overline{v} & \overline{\beta} \end{pmatrix}\begin{pmatrix} \gamma & w \\ -\overline{w} & \overline{\gamma} \end{pmatrix}$$

$$= a(xz) + b(yz)$$

En forma similar, obtenemos $x(ay + bz) = a(xy) + b(xz)$. Es decir, $\mathfrak{M}$ es una $\mathbb{R}$-álgebra.

Consideremos aplicación $h : \mathfrak{C} \to \mathfrak{M}$ definida por

$$h(\alpha e + u) = \begin{pmatrix} \alpha & u \\ -\,\overline{u} & \overline{\alpha} \end{pmatrix}.$$

Dados $x = (\alpha e + u), y = (\beta e + v) \in \mathfrak{C}$, $xy = [\alpha\beta - \langle \overline{u}, v\rangle]\, e + \overline{\alpha} v + \beta u + \overline{u} \times \overline{v}$.

$$\begin{aligned} h(xy) &= h\,(\,[\alpha\beta - \langle \overline{u}, v\rangle]\, e + \overline{\alpha} v + \beta u + \overline{u} \times \overline{v}\,) \\ &= \begin{pmatrix} \alpha\beta - \langle\, \overline{u}, v\rangle & \overline{\alpha}\, v + \beta u + \overline{u} \times \overline{v} \\ -\alpha\,\overline{v} - \overline{\beta}\,\overline{u} - u \times v & \overline{\alpha}\,\overline{\beta} - \langle u, \overline{v}\rangle \end{pmatrix} \\ &= \begin{pmatrix} \alpha & u \\ -\overline{u} & \overline{\alpha} \end{pmatrix}\begin{pmatrix} \beta & v \\ -\overline{v} & \overline{\beta} \end{pmatrix} \quad \text{(ver VII)} \\ &= h\,(\alpha e + u)\ h\,(\beta e + v) \end{aligned}$$

En consecuencia, h es un isomorfismo de $\mathbb{R}$-álgebras.

CONCLUSIONES

- Como consecuencia de la no conmutatividad de $\mathbb{H}$, los polinimios pueden tener más ceros que su grado. Por ejemplo los ceros de $x^2 + e$ son los cuaterniones puros $\mu = \beta i + \gamma j + \delta k$ tales que $\beta^2 + \gamma^2 + \delta^2 = 1$.

- El teorema de Frobenius garantiza que: Dada un álgebra $\mathcal{A}$ asociativa con elemento unidad $e \in \mathcal{A}$, sin divisores de cero; si la ecuación $x^2 + \beta x + \alpha e = 0$ tiene solución en $\mathcal{A}$, entonces $\mathcal{A}$ es isomorfa a $\mathbb{H}$.

- Toda álgebra real alternativa, cuadrática sin divisores de cero es isomorfa a $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ o $\mathbb{O}$.

Bibliografía

[1] Brenner, J. L. (1951). *Matrices of quaternions*, Pacific J. Math., 1 329-335.

[2] Curtis C. W., The Four and Eight Problem and Division Algebras, pp 100-125 of studies in Modern Algebra. Math. Assoc. of America 1963.

[3] Greub W.; Linear Algebra, Fourth Edition. Springer-Verlag, 1981.

[4] Herstein I. N.; Algebra Moderna. Editorial Trillas Mexico 1973.

[5] Kleinfeld E.; A characterization of the Cayley numbers, in Studies in Modern Analysis, MAA (1963), pp. 126-143.

[6] Koecher M., Remmert R.; Numbers. Graduate Texts in Mathematics. Readings in Mathematics. Springer, 1991.

[7] Munkres J. R.; Topología, segunda edición. Pearson Educación, S. A., 2002.

[8] Ogievetskii O. V.; A characteristic equation for 3x3 matrices over the octonions. (Russian) Uspekhi Mat. Nauk., **36** 197-198 (1981).

[9] Saltman J,; Lectures on Division Algebras. American Mathematical Society, 1999.

[10] Wiegmann N. A. Some theorems on matrices with real quaternion elements, Canad. J. Math., **7** 191-201 (1955)

[11] Wolf L. A.; Similerity of matrices in which the elements are real quaternions, Bull. Amer. Math. Soc., **42** 737-743 (1936)